JANUARY 2003

Defense Counsel Journal

Vol. 70 • No. 1 • Pages 1-184

The Privacy Project

Issued Quarterly by
IADC International Association of Defense Counsel

Defense Counsel Journal

January 2003
Volume 70, No. 1
Pages 1-184

International Association of Defense Counsel
Suite 2400
One North Franklin
Chicago, Illinois 60606-3401
Telephone (312) 368-1494
Fax (312) 368-1854
E-mail: info@iadclaw.org
Website: http://www.iadclaw.org

In this issue . . .

DEPARTMENTS

FEATURE ARTICLES

THE PRIVACY PROJECT

Defense Counsel Journal (ISSN: 0895-0016) is published quarterly (January, April, July, October) by the International Association of Defense Counsel, Suite 2400, One North Franklin, Chicago, Illinois 60606, telephone (312) 368-1494, fax (312) 368-1854, e-mail: office@iadclaw.org. Periodical postage paid at Chicago, IL, and additional mailing offices.

The subscription price of $65.00 annually is included in the dues of members of the IADC. POSTMASTER: Please send address changes to Defense Counsel Journal, Suite 2400, One North Franklin, Chicago, Illinois 60606.

Cite as: 70 DEF. COUNS. J. — (2003).

Defense Counsel Journal is a forum for the publication of topical and scholarly writings on the law, its development and reform, and on the practice of law, particularly from the viewpoint of the practitioner and litigator in the civil defense and insurance fields. The opinions and positions stated in signed material are those of the author and not by the fact of publication necessarily those of the International Association of Defense Counsel. Material accepted for publication becomes the property of the IADC and will be copyrighted as a work for hire. Contributing authors are requested and expected to disclose any financial, economic or professional interests or affiliations that may have influenced positions taken or advocated in the efforts.

Submit manuscripts to the Managing Editor at the above address in hard copy or via e-mail. *Defense Counsel Journal* follows *The Bluebook: A Uniform System of Citation* (17th ed.), and footnotes should be placed at the end of the article's text.

Officers and Executive Committee

OFFICERS

President, Joan Fullam Irick, Indianapolis, Indiana
President-Elect, J. Walter Sinclair, Boise, Idaho
Immediate Past President, William C. Cleveland III, Charleston, South Carolins
Vice-President, Kirk G. Forrest, Tulsa, Oklahoma
Vice-President, Lee L. Bennett, Baltimore, Maryland
Secretary-Treasurer, John G. Maxa, New Bremen, Ohio
Executive Director, Oliver P. Yandle, Chicago, Illinois

EXECUTIVE COMMITTEE

The President, the President-elect, the Vice-Presidents, the Secretary-Treasurer, and the following elected members:

Terms ending July 2003	**Terms ending July 2004**	**Terms ending July 2005**
George S. Hodges White Plains, New York	S. Stuart Clark Sydney, New South Wales	John S. Bradford Lake Charles, Louisiana
Christopher W. Tompkins Seattle, Washington	Cathy Havener Greer Denver, Colorado	Patrick Lysaught Kansas City, Missouri
Walter E. Zink II Lincoln Nebraksa	Gregory M. Lederer Cedar Rapids, Iowa	Bruce R. Parker Baltimore, Maryland

PAST PRESIDENTS

*Myron W. Van Auken	1920-1923
*Martin P. Cornelius	1923-1926
*Edwin A. Jones	1926-1932
*George W. Yancey	1932-1934
*Walter R. Mayne	1934-1935
*J. Roy Dickie	1935-1936
*Marion N. Chrestman	1936-1937
*P. E. Reeder	1937-1938
*Milo H. Crawford	1938-1939
*Gerald P. Hayes	1939-1940
*Oscar J. Brown	1940-1941
*Willis Smith	1941-1943
*Pat H. Eager Jr.	1943-1944
*F. B. Baylor	1944-1946
*Paul J. McGough	1946-1947
*Lowell White	1947-1948
*Kenneth P. Grubb	1948-1949
*L. Duncan Lloyd	1949-1950
*Wayne E. Stichter	1950-1951
*Joseph A. Spray	1951-1952
*Alvin R. Christovich	1952-1953
*J. A. Gooch	1953-1954
*Stanley C. Morris	1954-1955
*Lester P. Dodd	1955-1956
*John A. Kluwin	1956-1957
*Forrest A. Betts	1957-1958
*G. Arthur Blanchet	1958-1959
*Charles E. Pledger Jr.	1959-1960
Denman Moody	1960-1961
Payne Karr	1961-1962
*William E. Knepper	1962-1963
Richard W. Galiher	1963-1964
*Kraft W. Eidman	1964-1965
*Wallace E. Sedgwick	1965-1966
*Harley J. McNeal	1966-1967
*Egbert L. Haywood	1967-1968
*Gordon R. Close	1968-1969
*W. Ford Reese	1969-1970
*Samuel J. Powers Jr.	1970-1971
*Edward J. Kelly	1971-1972
Alston Jennings	1972-1973
Walter A. Steele	1973-1974
Theodore P. Shield	1974-1975
Jerry V. Walker	1975-1976
Henry Burnett	1976-1977
*Darrell L. Havener	1977-1978
Robert E. Leake Jr.	1978-1979
John R. Hoehl	1979-1980
Neil K. Quinn	1980-1981
William K. Christovich	1981-1982
Robert D. Norman	1982-1983
*Grant P. DuBois	1983-1984
*Thomas H. Sharp Jr.	1984-1985
*William H. Wallace	1985-1986
Henry B. Alsobrook Jr.	1986-1987
W. Richard Davis	1987-1988
George B. McGugin	1988-1989
*Morris R. Zucker	1989-1990
Jay H. Tressler	1990-1991
David J. Beck	1991-1992
Henry A. Hentemann	1992-1993
Michael A. Pope	1993-1994
Kevin J. Dunne	1994-1995
Edward J. Rice, Jr.	1995-1996
George Gore	1996-1997
Charles F. Preuss	1997-1998
Rex K. Linder	1998-1999
George H. Mitchell	1999-2000
Gregory C. Read	2000-2001
William C. Cleveland III	2001-2002

**Deceased*

President's Page

Introducing The Privacy Project

By Joan Fullam Irick

WHEN I was selected to serve as IADC President for the 2002-03 term, I decided to make the issue of corporate and personal privacy a key theme for my administration. Recent articles in newspapers, magazines and other media have been filled with "horror stories" of attacks on privacy rights, including in recent months:

- The county attorney of Buena Vista County, Iowa, subpoenaing the names of hundreds of women who had pregnancy tests at a local Planned Parenthood clinic as part of an investigation of the death of an unidentified baby.
- The 10 active federal trial judges in South Carolina voting unanimously to ban "secret legal settlements" on products liability, medical malpractice and other complex litigation.
- Administrators at an Ivy League college hacking into a rival university's computer system to obtain information about applicants for admission.

The issue of privacy is, of course, a touchy one. While we all have a strong desire to guard our own privacy and to protect ourselves from the undue curiosity of hackers, employers and overzealous neighbors, at the same time we want to know everything we possibly can about the backgrounds, criminal records and personal problems of those who live or work around us.

In July 2001, I presented to the IADC Executive Committee a written proposal for the creation of a Privacy Project to explore in depth recent changes in the privacy landscape, the current status of privacy on both the national and international scene, and the foreseeable future of privacy in the individual and corporate worlds. The Privacy Project was then submitted to the Institute of the IADC Foundation, which agreed to oversee and supervise the implementation of my proposal.

Over the past several months, a series of scholarly white papers have been authored by a number of talented and committed IADC members and partners and associates. Those papers are included in this issue of *Defense Counsel Journal* as the first stage of the Privacy Project.

Privacy will also be a key issue and a major topic of discussion at the IADC midyear meeting in February 2003 and the Corporate Counsel College in April 2003 in Chicago.

In the summer of 2003, a second and more expanded volume will be published by the IADC Foundation. In addition to the authors of the papers herein, the second volume will include many additional areas of study and discussion by a number of other IADC members.

I thank the individual authors and the *Defense Counsel Journal* editors for their efforts on behalf of the Privacy Project.

Calendar of Legal Organization Meetings

2003

February 5-11, American Bar Association Midyear Meeting, Seattle, Washington

February 15-20, IADC Midyear Meeting, The Inn at Spanish Bay, Pebble Beach, California

February 23-March 2, Federation of Defense and Corporate Counsel Winter Meeting, Westin Mission Hills Resort, Rancho Mirage, California

March 20-23, American College of Trial Lawyers Spring Meeting, Boca Raton Resort and Club, Boca Raton, Florida

April 8-13, Association of Defense Trial Attorneys Annual Meeting, Silverado Resort, Napa, California

April 22-25, IADC Corporate Counsel College, Ritz-Carlton Hotel, Chicago, Illinois

June 28-July 3, IADC Annual Meeting, Grand Wailea Resort and Spa, Maui, Hawaii

August 2-9, IADC Trial Academy, University of Colorado, Boulder

August 7-13, American Bar Association Annual Meeting, HQ: San Francisco Hilton, San Francisco, California

October 8-10, American Corporate Counsel Association Annual Meeting, San Francisco Marriott, San Francisco, California

October 15-19, Defense Research Institute Annual Meeting, Washington Hilton and Towers, Washington, D.C.

October, Product Liability Advisory Council Fall Meeting, TBA

October 29-November 1, American College of Trial Lawyers Annual Meeting, Fairmont Hotel, Montréal, Québec, Canada

2004

February 4-10, American Bar Association Midyear Meeting, San Antonio, Texas

February 7-12, IADC Midyear Meeting, The Cloister, Sea Island, Georgia

July 3-9, IADC Annual Meeting, The Homestead, Hot Springs, Virginia

August 5-11, American Bar Association Annual Meeting, Atlanta, Georgia

31st Annual
IADC Trial Academy

August 2-9, 2003

University of Colorado, Boulder, Colorado

The Academy is a program designed by the International Association of Defense Counsel to enhance the trial advocacy skills of younger lawyers who have been in practice from two to six years and have had actual trial experience.

Instruction in the major segments of trial are featured, including a wide variety of evidentiary problems. A seven-to-one student-faculty ratio enables faculty to critique each student's work.

Faculty demonstrations by leading defense trial lawyers and extensive use of videotape expose participants to different approaches and ideas in solving common trial problems. A physician will familiarize the students with the medical issues, and a segment on the testimony of an economist will also be featured.

Emphasis is placed on the learning-by-doing method of instruction. Individual students will cross-examine physicians and economists acting as expert witnesses and will be videotaped while participating in all aspects of trial. Students are given videotapes containing their presentations at the conclusion of the Academy.

Only a limited number of applicants can be accepted because of the trial concepts utilized. To request an application, contact the International Association of Defense Counsel, One North Franklin, Suite 2400, Chicago, Illinois 60606, at (312) 368-1494 and ask for Nancy Chase, Conference Coordinator. Fax: 312-368-1854. E-mail: nchase@iadclaw.org.

The Trial Academy qualifies for CLE credits in states with CLE accreditation. Last year, most students received approximately fifty-six hours of state CLE credit. Costs incurred for attending legal seminars which maintain and improve professional skills required for employment are tax deductible. See Treas. Reg. 1.162-5; IRS Letter Ruling 7746068 (9-1-77); Coughlin v. Comm'r, 203 F.2d 307.

Defense Counsel Journal

Back issues of *Defense Counsel Journal* are available from William S. Hein & Co., 1285 Main St., Buffalo, N.Y. 14209 ● *Defense Counsel Journal* is indexed in *Index to Legal Periodicals*, published by H.W. Wilson Co., 950 University Ave., Bronx, N.Y. 10452 and in *Current Law Index*, sponsored by American Association of Law Libraries and published by Information Access Co., 362 Lakeside Drive, Foster City, Calif. 94404 ● *Defense Counsel Journal* is available in microform from University Microfilms Inc., 300 Zeeb Road, Ann Arbor, Mich., and in CD-ROM form from ABI/Inform, also a service of University of Microfilms Inc. ● *Defense Counsel Journal* is included in the online and CD-ROM services of Westlaw, West Group, 610 Opperman Drive, Eagan, Minn. 55123, and in the database of Lexis, a service of Mead Data Central, 9393 Springboro Pike, Dayton, Ohio 45401 ● *Defense Counsel Journal* is listed in *Ulrich's International Periodicals Directory*, published by R.R. Bowker, 121 Chanlon Road, New Providence, N.J. 07974; in *Insurance Almanac*, published by Insurance Printing & Underwriting Co., 50 E. Palisade Ave., Englewood, N.J. 07631; in *Serials Directory: An International Reference Book*, published by EBSCO Industries Inc., Box 1943, Birmingham, Ala. 35201; in *INSURLAW/Insurance Periodicals Index Thesaurus & User's Guide*, published by NILS Publishing Co., P.O. Box 2507, Chatsworth, Calif. 91311; and in INFOSERV, an online service of Faxon Co., 15 Southwest Park, Westwood, Mass. 02090.

Announcing the 2003 International Association of Defense Counsel Legal Writing Contest

The IADC's annual legal Writing Contest is open to law students who at the time of the submission of their articles are enrolled in law schools approved by the American Bar Association or Canadian law schools listed in the Association of American Law Schools Directory. In order to inform members of this important activity and enlist their support in publicizing the contest, the rules of the competition are listed below.

IADC LEGAL WRITING CONTEST 2003 RULES

1. Eligibility. The International Association of Defense Counsel 2003 Legal Writing Contest is open to students who, at the time of submission of their entries, are enrolled in law schools accredited by the American Bar Association or in Canadian law schools listed in the Association of American Law Schools Directory.

2. Subject Matter. Entries must be submitted in the English language on a subject of practical concern to lawyers engaged in the defense or management of the defense of civil litigation, such as, for examples, relevant aspects of tort law, insurance law, civil procedure, evidence, damages, alternative dispute resolution procedures, and professional ethics.

3. Authorship and Publication. Entries must be certified by the entrant on the IADC entry form to be the original and sole work of the entrant. At the time of submission, the entry must not have been published or accepted for publication, and the author must be free to execute the assignment of copyright to IADC referred to in Rule 7.

4. Judging. The contest will be judged by a committee of the IADC, whose decisions will be final. In addition to the monetary award winners, the judges may designate entries worthy of honorable mention, but which will receive no monetary award.

5. Judging Standards. Articles will be judged on the following factors: (1) the choice of subject matter, as measured by its significance, international or national relevance, and timeliness; (2) the amount of work and effort, as measured by the entry's comprehensiveness and analysis; (3) the quality of the legal analysis, as measured by its objectivity and balance; and (4) the writing quality, as measured by clarity of expression, brevity, and literary construction. Entrants also should consider the points made in the contest guidelines.

6. Monetary Awards. Monetary awards will be made as follows: US$2,000 to first place, US$1,000 to second place, and US$500 to third place.

7. Plaques and Publication. Authors of monetary award articles and of those awarded honorable mention will receive commemorative plaques, and their articles will be made available for publication in *Defense Counsel Journal*, IADC's quarterly law review. At the time of submission, entrants must execute the assignment of copyright in the entry certificate. IADC will copyright articles published in *Defense Counsel Journal*, but will release the copyright assignment back to entrants whose works are not published. Acceptance for publication in any publication other than *Defense Counsel Journal* prior to notice to the author of an award in this contest will disqualify the entry. Entrants are expected to notify IADC promptly of such prior acceptance by another publication.

8. Subscription. A year's subscription to *Defense Counsel Journal* will be given to all contestants who meet the qualifications for entry in this contest.

9. Deadline for 2003 Entries. If transmitted by mail, entries must be postmarked on or before April 16, 2003. If transmitted other than by mail, they must be received on or before that date.

10. Directions for Transmission. Entries, together with the completed entry form, must be transmitted to the International Association of Defense Counsel, One North Franklin, Suite 2400, Chicago, IL 60606-3401.

Contest announcement, rules, writing guidelines, and entry forms are available at http://www.iadclaw.org

International Association of Defense Counsel Tenets of Professionalism

1. We will conduct ourselves before the court in a manner which demonstrates respect for the law and preserves the decorum and integrity of the judicial process.

2. We recognize that professional courtesy is consistent with zealous advocacy. We will be civil and courteous to all with whom we come in contact and will endeavor to maintain a collegial relationship with our adversaries.

3. We will cooperate with opposing counsel when scheduling conflicts arise and calendar changes become necessary. We will also agree to opposing counsel's request for reasonable extensions of time when the legitimate interests of our clients will not be adversely affected.

4. We will keep our clients well informed and involved in making the decisions that affect their interests, while, at the same time, avoiding emotional attachment to our clients and their activities which might impair our ability to render objective and independent advice.

5. We will counsel our clients, in appropriate cases, that initiating or engaging in settlement discussions is consistent with zealous and effective representation.

6. We will attempt to resolve matters as expeditiously and economically as possible.

7. We will honor all promises or commitments, whether oral or in writing, and strive to build a reputation for dignity, honesty and integrity.

8. We will not make groundless accusations of impropriety or attribute bad motives to other attorneys without good cause.

9. We will not engage in discovery practices or any other course of conduct designed to harass the opposing party or cause needless delay.

10. We will seek sanctions against another attorney only when fully justified by the circumstances and necessary to protect a client's lawful interests, and never for mere tactical advantage.

11. We will not permit business concerns to undermine or corrupt our professional obligations.

12. We will strive to expand our knowledge of the law and to achieve and maintain proficiency in our areas of practice.

13. We are aware of the need to preserve the image of the legal profession in the eyes of the public and will support programs and activities that educate the public about the law and the legal system.

The Privacy Project

In 2001, Joan Irick submitted a proposal for consideration to the IADC Executive Committee concerning a new project for the Institute of the IADC Foundation. The proposal was accepted immediately by the Executive Committee as an important emerging area of law that warranted further inquiry. The IADC Foundation Board agreed, and the idea grew into the Privacy Project.

The IADC Foundation turned to Board Member George S. Hodges, who agreed to chair an editorial team that would bring the Privacy Project from concept into a form that would benefit the IADC membership and legal community. Joining him were Joseph W. Ryan Jr. and Jerome A. Galante.

A plan was implemented to research and organize every conceivable legal topic dealing with privacy. Once the list was complete, a plan developed to create a series of scholarly white papers on each privacy topic. Authors from within the IADC ranks were chosen. Each agreed to submit a paper on a specified area of privacy within a very strict timetable. Commitment to a specific topic, submission of initial outlines, drafts and final drafts were carefully coordinated during countless telephone conferences and e-mails among the editorial board, authors and IADC staff.

The goal was to have publishable material in the hands of Richard B. Allen, Managing Editor of *Defense Counsel Journal*, for publication in the January 2003 issue. Holding to this tight time table would allow the IADC membership an opportunity to read the scholarly papers before the February 2003 IADC midyear meeting in Pebble Beach, which has privacy as its theme.

The Privacy Project editorial team thanks the authors for their commitment and dedication to this project. In particular, Kathy Blaner, Bob Curley, Ralph Streza, George Hodges, Eric Wiechmann, Bill Porter, Becky Wilson, Mark Fox, Laurel Harbour, Stu Clark and Nancy Lawson. The talent and dedication of these individuals form the cornerstone of this project.

The editorial team also thanks Pam Miczuga of the IADC staff, who assisted with scheduling numerous telephone conferences, then quickly and efficiently published and distributed the minutes of the meetings, and IADC Executive Director Oliver Yandle for his thoughtful suggestions and input. Finally, the editorial team thanks IADC President Joan Irick, who brought her idea to the Executive Committee, which in turn provided the IADC Foundation an opportunity to sponsor a project that will improve the legal community's understanding of privacy issues.

The Privacy Project

The Emperor Has No Clothes: How Courts Deny Protection for Confidential Information

Litigants' rights to protection of information not used in judicial proceedings should trump any public right to access

By Kathleen L. Blaner

THROUGHOUT the centuries, fairy tales have provided valuable lessons about human nature and have given us surprising insights into complex adult transactions. One story, about the emperor's new clothes, sheds significant light on an ongoing controversy about whether information produced in the preliminary stages of civil litigation should be kept confidential when it is not used in court.

In the fairy tale, several entrepreneurial tailors trick the emperor into believing that they have designed the most exquisite clothing ever made for royalty. In reality, the tailors have fashioned nothing. To demonstrate his acute, discerning judgment and his great vision to the people he rules, the emperor claims to see the "exquisite garments" that the trickster tailors pretend to parade before them. The emperor's advisors are afraid to tell him there is nothing there. The tailors pretend to measure and fit the "garments" just as if they had real cloth in their hands. No one is willing to admit that there is nothing in the tailors' hands and that, when the emperor "puts on" the garments, the emperor is wearing no clothes.

IADC member Kathleen L. Blaner is chair of the IADC Legislative, Judicial and Governmental Affairs Committee, co-chair of the State Law Subcommittee of the American Bar Association Litigation Section Class Action and Derivative Suits Committee, serves on the Executive Committee of Lawyers for Civil Justice, and is a consultant to Covington & Burling. She is a graduate of American University (A.B. 1978) and Catholic University Law School (J.D. 1989).

THE NEW FAIRY TALE

This tale parallels how courts have reacted to the protective order and confidential settlement controversy over the last decade.[1] Some members of the media and the organized plaintiffs bar claim that confidentiality orders entered in litigation have concealed horrific defects in products that have killed hundreds or have kept secret corporate misdeeds that have caused unconscionable harm.[2] Others, including the research arm of the United States Judicial Conference and the chair of the conference's Advisory Committee on Civil Rules have tried to point out that the facts alleged simply do not support the claims.[3]

1. *See generally* Martha Neil, *Confidential Settlements Scrutinized,* A.B.A. J. July 2002 at 20-22; Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427 (1991); Richard L. Marcus, *The Discovery Confidentiality Controversy*, 1991 U. ILL. L. REV. 457, 459; Arthur R. Miller, *Private Lives or Public Access?* A.B.A. J., August 1991, at 65; Arthur R. Miller, *Memorandum to the New York State Office of Court Administration on Proposed Rule 216.1 Regarding the Sealing of Court Records* at 3-7 (December 10, 1990).

2. Neil, *supra* note 1. *See also* Letter dated June 24, 2002, from Chief Judge Joseph F. Anderson Jr. of the U.S. District Court for the District of South Carolina, requesting the district judges to adopt a court rule to preclude confidential settlements; Scott Bundgaard, member of the Arizona State Senate, *Petition under Rule 28 of Rules of the Arizona Supreme Court*, filed January 30, 2002.

3. *See, e.g.*, Federal Judicial Center, *Report on Protective Order Practice* (1996).

Despite the lack of real substance to the claims, over the last decade it has become increasingly difficult to protect confidential information produced in discovery in civil litigation. Many courts no longer allow parties to a lawsuit to stipulate to a protective order providing blanket protection against public disclosure for information that implicates privacy or property rights. Instead, they insist on a document-by-document review of the thousands—indeed, tens of thousands—of pages often produced in complex litigation, regardless of whether that information will ever be found sufficiently relevant to use in actual court proceedings.[4]

Courts also are increasingly refusing to allow litigants to settle legal claims conditioned on a promise that the settlement will be kept confidential.[5] Even a non-substantive order of dismissal that follows the parties' agreement to settle a dispute becomes a triggering device that courts use to justify disclosure of information produced in the embryonic stages of litigation.[6] Recent decisions from the U.S. Court of Appeals for the Seventh Circuit place litigants in an untenable catch-22 position. A settlement will remain confidential only if is never approved by the court. However, if it is never approved by the court, the parties lack the ability to seek enforcement of the agreement if one fails to comply.

FORGETTING THE LITIGANTS

It seems as if courts have forgotten that litigants have rights at stake in the protective order controversy—or, at least, courts are giving them very little attention. Yet the privacy and property rights implicated in information in today's world have assumed transcendent importance to society, just as the protective order debate has raged most fiercely.[7] The rapid growth of electronic communications has placed personal privacy high on the endangered species list. The development and protection of intellectual property related to electronic commerce, as well as more traditional forms of commercial activity involving trade secrets, are among the paramount concerns of most businesses.[8] A company's proprietary interest in its intellectual property may often be that company's most valuable asset.

At a time when the need for confidentiality is greater than ever before for both private individuals and the business community, the courts are less likely to provide assurances that information produced in litigation will be kept confidential and protected.[9] This paradox, wherein courts refuse to protect what now requires the highest levels of protection, is the result of a systematic campaign by the organized plaintiffs bar and the communications media over the last 15 to 20 years.

These two groups have somehow convinced many courts, both state and federal, into believing that there is a problem that needs to be fixed. They have made some courts believe that courts can and should be champions of the public welfare through the active dissemination of confidential in-

---

4. *See, e.g.*, Chicago Tribune Co. v. Bridgestone/Firestone Inc., 263 F.3d 1304, 1314-15 (11th Cir. 2001).

5. *See, e.g.*, Jessup v. Luther, 277 F.3d 926 (7th Cir. 2002); In re Adams v. City of Lebanon, available at http://caselaw.lp.findlaw.com/data2/tennesseestatecases/appeals/2002_1/adamsjohn.pdf, *rehearing denied*, 2002 Tenn.App. Lexis 123 (court lacks jurisdiction to issue protective oeder when there is no action before it).

6. *See, e.g.*, Herrnreiter v. Chicago Housing Authority, 281 F.3d 634 (7th Cir. 2002) (motion to file documents under seal denied; appellate papers placed in public record) (ruling below, 2001 U.S.Dist. Lexis 11071 (N.D. Ill.); Jessup, 277 F.3d at 929 (court's approval of dismissal of action and placing settlement agreement in court files, even when sealed, are public acts subject to public disclosure).

7. *See* Pamela Samuelson, *Information as Property: Do Ruckleshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?* 38 CATH. U. L. REV. 365, 367 (1989) (discussing whether information age requires change in how law treats information).

8. *See* Gregory Gelfand, *Taking Informational Property Through Discovery*, 66 WASH. U. L.Q. 703 (1988)

9. Jessup, 277 F.3d at 929 (recognizing importance of confidentiality to trade secrets, personal privacy and confidential settlements nothwithstanding order upholding disclosure of confidential settlement in specific case).

formation, although the information was exchanged between private parties to resolve private, civil legal disputes. They have convinced courts to believe and act as if this role somehow trumps the courts' obligation to serve as a neutral arbiter of legal disputes. Courts have reacted to horror stories in the media about "court secrecy" and have give greater credence to public opinion based on bald allegations than to documented claims of privilege and confidentiality.

Fortunately for society, the claims of the plaintiffs bar and the media have been investigated by judicial officers and scholars and been called "unfounded."[10] Indeed, this emperor has no clothes. But unfortunately for many parties who have been hauled into court against their will and compelled to produce highly confidential information, courts have acted as if the claims were true. The truth is that there is no problem that needs to be addressed and nothing that warrants changes in legislation or court rules.

NOT A ROLE FOR COURTS

No matter how strongly they believe to the contrary, courts rarely, if ever, are meaningful resources for warning the public about imminent public health risks, active environmental hazards or other pending threats to the public welfare. By the time a dispute gets into a court, any threat to the public has been or could have been made known to the public through a variety of other means. Usually there is immediate media coverage of even the most nascent suggestion that a consumer product, corporate conduct, environmental incident or government action is potentially harmful or wrong. Regulatory agencies, local governments and the media are far better suited to providing information to the public.

In a number of cases, the initial media claims and lawsuits have had no scientific basis. Good products and businesses have been unfairly taken off the market or driven out of business.[11] That was the fate of the Audi 5000 automobile and the Dow Corning breast implants. Both products were needlessly withdrawn from the market following massive media campaigns and thousands of lawsuits in which protective orders were involved. Scientific evidence eventually vindicated both products, but that came too late. Women had thousands of unnecessary operations to remove the implants alleged to be harmful. Dow Corning went into bankruptcy as a result of the litigation. The market for Audi products in the United States was devastated for years, and Audi and Audi owners suffered irreparable financial loss.[12]

In the recent controversy over Firestone tires, a *New York Times* article exposed the fact that the plaintiffs' lawyers themselves had concealed information about accidents involving the tires from the appropriate regulatory agency in order to have better control of the litigation and garner higher settlement awards.[13] Contrary to the claims that Bridgestone/Firestone hid vital information from the public, the 11th Circuit found that Firestone actually had produced trade secrets in the litigation which warranted a confidentiality order.[14]

---

10. *See* Federal Judicial Center report, *supra* note 3. *See also* Letter dated March 23, 1998, from Paul V. Niemeyer, Judge of the U.S. Court of Appeals for the Fourth Circuit and then chair of the Judicial Conference Advisory Committee on Civil Rules, to the Representative Henry J. Hyde, chair of the U.S. House Judiciary Committee; Miller, 105 HARV. L. REV., *supra* note 1.

11. *See* Ealy v. Richardson-Merrell Inc., 897 F.2d 1159 (D.C. Cir.), *cert. denied*, 498 U.S. 950 (1990) (no scientific basis for claim that Bendectin caused birth defects, yet Bendectin removed from market because of liability costs); Walter Olson, *No Secrets*, REASON, February 1991, at 25.

12. *See* Peter Huber, *Manufacturing the Audi Scare*, WALL ST. J., December 18, 1989, at A18 (no truth to claim that Audi 5000 was subject to sudden acceleration).

13. Keith Bratsher, *S.U.V. Tire Defects Were Known in '96 But Not Reported*, N.Y. TIMES, June 24, 2001, at A1.

14. 263 F.3d at 1314-15.

CAMPAIGN IN THE STATES

When the protective order controversy began in the early 1990s, more than half of the states considered legislation or court rules to restrict the use of protective orders and confidentiality agreements. In 1991, 28 states considered but did not enact restrictive legislation of this type.[15] The same year, four states considered rules changes, but only two—New York and Delaware—put them into effect. Two states—Florida and Texas—in 1990 enacted changes that appeared likely to place heavy restrictions on the availability of protective orders, particularly in product liability litigation.[16]

Section 69.081(4) of the Florida statute states:

> (4) Any portion of an agreement or contract which has the purpose or effect of concealing a public hazard, any information concerning a public hazard, or any information which may be useful to members of the public in protecting themselves from injury which may result from the public hazard, is void, contrary to public policy, and may not be enforced.

Texas Rule of Civil Procedure 76a states that "court records . . . are presumed to be open to the general public," and it defines "court records" as, among other things, "discovery, not filed of record, concerning matters that have a probable adverse effect upon the general public health and safety."

In practice, however, the Texas restrictions have not had the effect their supporters intended. Courts have interpreted the changes in ways that preserve judicial discretion to protect confidential information.[17]

From the early 1990s to 2000, the frenzy in state legislatures over protective orders and confidentiality quieted down. The proponents of restrictions on protective orders and confidential settlement agreements turned to Congress and federal rule makers to make their claims, but ultimately they were unsuccessful.[18]

Undeterred, the proponents of restrictions on protective orders and confidentiality agreements returned to the states. In the 2001-02 legislative sessions, no less than 22 bills were introduced to limit the use of confidentiality in civil litigation. Legislation was considered in Arizona (S.B. 1453), California (S.B. 11 and A.B. 36), Connecticut (S.B. 625), Hawaii (H.B. 1350), Illinois (H.B. 75, 156, 3146 and 4277), Massachusetts (S.B. 862), Missouri (S.B. 686 and 1021), New York (A.B. 7513 and 1066), North Carolina (S.B. 1071), Oklahoma (S.B. 1555), Rhode Island (H.B. 5617 and 6613, S.B. 194 and 2707) and Tennessee (H.B. 1216 and S.B. 1175). Although bills in a number of states had significant momentum toward passage at various times, none had been enacted by October 2002.

In general, the proposed legislation and court rules are aimed at increasing public access in discovery and settlement, and almost every one was modeled after the Florida statute or the Texas court rule. The drafters anchor their proposals in the states' inherent police powers to regulate public health, safety and welfare, thereby attempting to justify the public access requirement as a necessary exercise of state police power.[19] But the 1991 California proposals also included personal injury and wrongful death actions.

---

15. Alabama, Alaska, Arkansas, California, Colorado, Connecticut, Hawaii, I11inois, Iowa, Kansas, Louisiana, Maine, Massachusetts, Minnesota, Mississippi, Montana, Nevada, New Hampshire, New Jersey, New Mexico, New York, Oregon, Pennsylvania, Rhode Island, South Dakota, Virginia, Washington and Wisconsin.

16. FLA. STAT. ANN. § 69.081 and TEX. R. CIV. P. ANN. r. 76a.

17. *See, e.g.,* Ford Motor Co. v. Benson, 846 S.W.2d 487 (Tex.App.—Houston 1993) (interpreting rule to require plaintiff to prove documents affect public health and safety, thereby triggering restriction on protective orders); Eli Lilly K& Co. v. Biffle, 868 S.W.2d 806 (Tex.App.—Dallas 1991) (issuing mandamus to direct trial court to interpret new rule to protect trade secrets).

18. *See* Niemeyer letter, *supra* note 10; Arthur R. Miller, *Protective Order Practice: No Need to Amend F.R.C.P. 26(c)*, PROD. LIAB. REP. (CCH), April 21, 1995 at 438-39.

19. *See generally* RICHARD A. EPSTEIN, TAKINGS 107-45 (1985) (discussing the origins and nature of inherent police powers of state).

Following the Florida and Texas standards, courts could not issue protective orders or seal court records if doing so would have the purpose or effect of "concealing a public hazard or information concerning a public hazard," to quote the Alaska bill, or if doing so "concerns matters that have a probable adverse effect upon the general public health or safety," the Illinois formulation. In recent years, some legislatures, particularly California, have expanded the definition to also include disclosure of information concerning "environmental hazards" and "financial fraud."

Several of the 1991 introductions—for instance, Alaska, Arkansas, Kansas, Montana and South Dakota—defined "public hazard" as "an instrumentality, including but not limited to any device, instrument, person, procedure, product, or a condition of a device, instrument, person, procedure, or product, that has caused and is likely to cause injury." This definition is remarkably broad and could easily encompass much more than some potential injury to public health and safety. Accessibility would be required without regard for whether the information was contained in records filed with the court, kept in the private offices of the litigants themselves, or in the hands of third parties.

Whether the information was gleaned through discovery or document production and ultimately would not be filed with the court or used at trial would be immaterial.[20] This is contrary to legal tradition, which has always recognized the admission of evidence at trial as the "touchstone" of the public's right to access.[21]

Most of the proposed legislation also would allow members of the media and the general public to intervene in litigation for the sole purpose of obtaining access to confidential information that was produced subject to a protective order, confidentiality agreement or court sealing. Both the California and Illinois introductions accord standing to "any person."

Recent actions in South Carolina and Arizona are much more problematic. In August 2002, the federal district judges of the District of South Carolina, at the behest of Chief Judge Joseph F. Anderson Jr., announced the adoption of a new provision to Local Rule 5.03 stating, "No settlement agreement filed with the court shall be sealed pursuant to the terms of this rule." But the court also stated that it would receive comments until September 30, 2002, after which it would announce any "necessary" modification. A large volume of comments was received from South Carolina, as well as out-of-state lawyers and national organizations. Unmoved by the comments, on November 6, 2002, the court announced adoption and implementation of the new amended rule.[22] Not to be left behind, Chief Justice Jean Toal of the South

---

20. *See* In re Reporters Comm. for Freedom of the Press, 773 F.2d 1325, 1338 (D.C. Cir. 1985), in which then Judge Scalia analyzed the historical practice of courts regarding public access to court records, relying heavily on decisions from the Supreme Court of Michigan, Schmedding v. May, 48 N.W. 201 (Mich. 1891), and the Massachusetts Supreme Judicial Court, Cowley v. Pulsifer, 137 Mass. 392 (1884). In Cowley, the court said, "[I]t is clear that [these grounds] have no application whatever to the contents of a preliminary written statement of a claim or charge. These do not constitute proceedings in open court. Knowledge of them throws no light upon the administration of justice. Both form and contents depend wholly on the will of a private individual, who may not even be an officer of the court." 137 Mass. at 394. According to Judge Scalia, in order to accept a public right of access to prejudgment records, "one would have to accept that the court, writing in the days before photostatic copying, envisioned the passing around of documentary exhibits from the jury to the audience, or the manual copying of all of them." 773 F.2d at 1334-35 n. 7.

21. Reporters Comm., 773 F.2d at 1338.

22. The notice of adoption of rule and the rule are available on the court's website—www.scd.uscourts.gov/rules/aug2001/cv/ch5.pdf, and the comments are available at www.scd.uscourts.gov/Notices/COMLR503.pdf. The announcement of adoption of the amendment to Rule 5.03 is available at www.scd.uscourts.gov/Notices/LR503.pdf. *See also* Adam Liptak, *In South Carolina, Judges Seek to Ban Secret Settlements*, N.Y. TIMES, September 2, 2002, at A1. The *New York Times* was quick not only to endorse the South Carolina initiative but also to speak favorably of barring parties and attorneys from participating in "secret settlements." *See* Editorial, *Ending Legal Secrecy*, N.Y. TIMES, September 5, 2002, at A22.

Carolina stated that she favored barring "secret settlements" in South Carolina state courts.[23]

In January 2002, Scott Bundgaard, a member of the Arizona State Senate, petitioned that state's supreme court to consider adopting a court rule that would restrict the use of protective orders.[24]

Proposed legislation in California would do away with the traditional "good cause" standard for obtaining a protective order. Instead, it would require the court to balance the interest of the public in having access to the confidential information against the need for confidentiality. Only if the litigant's confidentiality claim passes the highest level of judicial scrutiny—that is, it demonstrates a compelling interest in confidentiality that overcomes the public's interest in access—will a protective order issue.

Yet it still is black-letter law under the U.S. Supreme Court's decision in *Seattle Times Co. v. Rhinehart*,[25] that there is no right of public access to information produced in civil discovery. The exact language of the Court used is, "A litigant has no First Amendment right of access to information made available only for purposes of trying his suit." This holding means that non-parties, including the public and the media, have no First Amendment right to obtain access to information produced in civil discovery.[26] The standard applied in much of the proposed legislation and rules reverses the presumption recognized under *Seattle Times* that the public has no right of access to material produced in discovery. Instead, it gives the public a greater right to the information than the litigants who own and produce the information.

These legislative and rule-making activities are highly troubling and unnecessary. Courts already have the inherent authority to control their own records, which includes the discretion to keep information confidential or to make it public.[27] Just as important, the courts already are some of the most open governmental institutions in the United States.[28] By common law tradition, civil and criminal trials, and the records filed with the court and used at trial or in judicial proceedings, are open to the public almost without exception.[29] The only areas that have been protected and that should remain subject to protection are areas at the periphery—information produced in discovery and included in confidential settlements. There is no tradition of public access to prejudgment, or discovery records in civil cases.[30]

---

23. Rick Brundrett, *Toal Backs Publicizing Lawsuit Settlements*, THE STATE [Columbia, South Carolina], August 7, 2002, at A5; Rick Brundrett, *Toal: Secret Deals Often Break Rules*, THE STATE [Columbia, South Carolina], August 23, 2002, at B3.

24. Supreme Court No. R-02-0002, Petition under Rule 28 of Rules of the Arizona Supreme Court, filed January 30, 2002. Comments were due by August 1, 2002, but no action had been taken by December 1, 2002. *See* www.supreme.state.az.us/rules/prrulciv.htm

25. 467 U.S. 20 (1984), *aff'g* 654 P.2d 673 (Wash. 1982).

26. In re Alexander Grant & Co. Litig., 820 F.2d 352, 355 (11th Cir. 1987), *aff'g* 629 F.Supp. 593 (S.D. Fla. 1986); Reporters Comm., 773 F.2d at 1339. *See also* Cippollone v. Liggett Group Inc., 785 F.2d 1108, 1119 (3rd Cir. 1986) (no First Amendment analysis required to determine whether protective order can bar public dissemination of discovery information); Worrell Newspapers of Indiana Inc. v. Westhafer, 739 F.2d 1219 (7th Cir. 1984), *rev'g* 570 F.Supp. 1447 (S.D. Ind. 1983) (no First Amendment analysis required); Phillips v. Gen. Motors Corp., 2002 U.S.App. Lexis 21489 (9th Cir.), *amending* 289 F.3d 1117, *vacating and remanding* 126 F.Supp.2d 1328 (D. Wash. 2001) (no common right of access to documents filed under seal; First Amendment not sufficiently raised).

27. Nixon v. Warner Communications Inc., 435 U.S. 589, 598 (1978).

28. Arthur R. Miller, *Private Lives or Public Access?* A.B.A.J., August 1991, at 65; Schmedding, 48 N.W. at 202.

29. The United States has a common law tradition of holding public trials. *See* Richmond Newspapers Inc. v. Virginia, 448 U.S. 555 (1980); Brown & Williamson Tobacco Corp. v. Fed. Trade Comm'n, 710 F.2d 1165, 1177-79 (6th Cir. 1983), *cert. denied*, 465 U.S. 1100 (1984); Marcus, *Confidentiality Controversy*, *supra* note 1, at 459.

30. Reporters Comm., 773 F.2d at 1334-39. Nonetheless, at one time some federal circuit courts held to the contrary. *See* Seattle Times, 467 U.S. at 25; In re Halkin, 598 F.2d 176 (D.C. Cir. 1979) (protective order can act as prior restraint on litigant's First Amendment right to free speech); In re San Juan Star Co., 662 F.2d 108 (1st Cir. 1981) (protective order is not prior restraint but does implicate First Amendment interests). *But see* Int'l Products

THE DISCOVERY PROCESS

Discovery is a relatively new invention, unknown prior to the adoption of the Federal Rules of Civil Procedure in 1938. The invasive nature of litigation today results largely from the modern discovery process, which requires the production of information, even if it will be inadmissible in the underlying action, as long as it is likely to lead to the production of admissible information. In its present incarnation, Rule 26(a) requires initial disclosures of certain information without a discovery request. As recently as 1970, parties were required to show good cause before a court would compel discovery. In a complete reversal, the rules now require production unless a party can show good cause not to produce.[31]

Surely, the founding fathers of the United States, who believed strongly in public trials, never imagined that preliminary, private information produced solely to facilitate resolution of the lawsuit would be universally available to any and all takers, particularly when it did not have the benefit of being found relevant to the underlying issues.[32] It follows that when discovery information results in a confidential settlement, the information retains its confidential nature unless used in court proceedings or introduced into court files.[33]

The discovery process and civil litigation as contemplated under the Federal Rules and the rules of most states envision the free flowing exchange of information in discovery between litigants in order to promote the early resolution of the dispute. When litigants fear that confidential information will not be protected, they will not be forthcoming in producing it. Discovery disputes will proliferate, making it necessary for already overburdened courts to mediate the pretrial process at a time when it was designed to be self-executing.

CONSTITUTIONAL DUTY TO PROTECT LITIGANT RIGHTS

In all the emotional rhetoric about the public's right to know, "secret settlements" and "court secrecy," the proponents of restrictions on protective orders and confidential settlements seem to ignore the fact that litigants also have rights. Often these rights reside in the information that must be produced under highly invasive modern discovery rules in order to resolve the underlying legal dispute. Consequently, efforts to increase public access to information related to litigation are in significant tension with the litigants' need to protect confidential information from disclosure. Only confidentiality protects the rights bound up in the information, rights which may be of constitutional stature.

Although this tension always has existed to some extent, its dynamics have undergone a profound metamorphosis in the last few decades as technological advances have moved society into the information age, where information itself is often an end product. Because of this transformation, ensuring strong legal protection for information is of much greater importance today than ever before.

Corp. v. Koons, 325 F.2d 403 2d Cir. 1963) (no First Amendment restriction on dissemination of information produced in litigation). *See also* Richard L. Marcus, *Myth and Reality in Protective Order Litigation*, 69 CORNELL L. REV. 1 (1983) (discussing lower court cases prior to Seattle Times). Any doubts about public access rights to civil iscovery, and whether they are grounded in the U.S. Constitution, were put to rest by Seattle Times.

31. William W. Schwarzer, *The Federal Rules, the Adversary Process and Discovery Reform*, 50 U. PITT. L. REV. 703 (1989). In recent years, leading scholars and jurists have recognized the abuse and excess bred by the current rules. *See, e.g.*, William W. Schwarzer, *Slaying the Monsters of Cost and Delay: Would Disclosure Be More Effective than Discovery?*, 74 JUDICATURE 178 (1991); Frank H. Easterbrook, *Discovery as Abuse*, 69 B.U. L. REV. 635, 645 (1989); Maurice Rosenberg & Warren R. King, *Curbing Discovery Abuse in Civil Litigation: Enough Is Enough*, 1981 BYU L. REV. 579; Wayne D. Brazil, *The Adversary Character of Civil Discovery: A Critique and Proposals for Change*, 31 VAND. L. REV. 1295 (1978).

32. See Reporters Comm., 773 F.2d at 1334-39 (discussing historical treatment of prejudgment records in civil proceedings).

33. *See* Luther, 277 F.3d at 928 (recognizing that even entire trial record may be sealed and citing supporting cases recognizing continued validity of confidentiality in litigation).

A. Property Rights in Information

Information is intangible property, and the U.S. Supreme Court has recognized explicitly that information, such as trade secrets and confidential business information, is a form of property.[34] To the founding fathers, who were steeped in Lockean theory, securing private property against theft and government confiscation or misappropriation was one of the most fundamental responsibilities of government. The Fifth Amendment to the Constitution, which guarantees a number of rights, contains the "takings clause," which states that "nor shall private property be taken for public use, without just compensation." Protecting private property was, therefore, one of the driving forces behind the initial break between the colonies and Great Britain, and it retains its vitality today.[35]

An owner of private property is said to possess a "bundle of rights" in the property. One stick in this bundle is the right to exclusive possession of the property.[36] The right to exclusive possession is often of transcendent importance when the property at issue is information. Unlike tangible or real property, informational property can be possessed simultaneously by more than one person. Thus, the basic value of informational property often is dependent on its exclusive possession or on confidentiality. If everyone knew the formula for Coca-Cola, for example, the Coca-Cola Co. would have no special advantage over any other soft drink manufacturer.

Other sticks within the bundle of property rights include the right to control the use and ultimate disposition of property. Again, these rights are of paramount importance when the property is information, because the owner can derive value from licensing the use of, or selling, exclusive information. Unlike tangible or real property, which can be disposed of only once, the same information can be sold over and over again without diminishing its original value, as evidenced by the market for computer programs or legal research services. If others can obtain the same information without paying for it, the potential value that can be derived from licensing or selling the original information is substantially, if not entirely, diminished.

When a court orders a litigant to produce proprietary information in litigation and to disclose that information to an opponent, the court's interference with the rights to exclusive possession and use of that information is immediately apparent. This interference can be tolerated when the court exercises its authority under existing law to prevent further disclosure outside of the lawsuit, either through the issuance of a protective order or by sealing the information in court files.

The degree of interference would increase exponentially, however, perhaps to the point of destroying the underlying property right, if the information disclosed in a limited manner to the court and the opponent is further disclosed to the general public, as would be required under the proposed legislation and court rules. Consequently, placing restrictions on or eliminating the court's authority to protect the confidentiality of proprietary information produced in litigation places property rights in information at serious risk of loss.

B. Right to Privacy in Information

Another right of constitutional significance often embodied in information is the right to privacy.[37] Although the right to pri-

---

34. Carpenter v. United States, 484 U.S. 19, 25-26 (1987), *aff'g* 791 F.2d 1024 (2d Cir. 1986) (newspaper's prepublication material is property); Ruckelshaus v. Monsanto Co, 467 U.S. 986, 1003-04 (1984), *vacating and remanding* 564 F. Supp. 552 (E.D. Mo. 1983) (trade secrets are property); Dirks v. Sec. Exch. Comm'n, 463 U.S. 646, 653 n.10 (1983) (confidential business information is property); Bd. of Trade of Chicago v. Christie Grain & Stock Co., 198 U.S. 236, 250-51 (1905), *aff'g* 130 F. 507 (7th Cir. 1904), *rev'g* 125 F. 161 (8th Cir. 1903) (futures exchange's price information protected by law). *See also* Samuelson, *Information as Property*, *supra* note 7.

35. EPSTEIN, *supra* note 20, at 16-17.

36. *See generally id*., at 58-62.

37. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536 (1982)

vacy is most often thought of as it relates to individual autonomy over certain personal decisions, the Supreme Court has recognized a second branch of privacy that may guarantee the right to avoid government disclosure to the public of certain private or personal information.

The Court has recognized several types of information that an individual or corporation may have an interest in preventing the government from disclosing, including: personal information collected while in public office,[38] identification of an individual as a user of prescription narcotics,[39] erroneous description of an individual as a drunkard,[40] erroneous description of a company as "lacking integrity,"[41] description of an individual as suicidal,[42] and information about a prior arrest or criminal record.[43]

The concern in most of these cases is not so much the risk that the information disclosed will be erroneous or otherwise likely to stigmatize the individual or organization to whom it pertains, although those are issues in these cases, but rather that disclosure will cause the individual some further detriment or loss beyond the erroneous stigmatization or loss of reputation.

Again, it is immediately apparent that if legislatures or rule makers restrict the authority of courts to protect information in which there may be a privacy right or interest, that action may result in the unwarranted public disclosure of information that not only injures the reputation of the individual to whom the information pertains, but that also triggers other detrimental consequences. One can easily imagine how this damage could occur, especially in light of some telling examples already discussed, such as the Audi 5000 and breast implants, in which premature publication of confidential can inflict serious injury.

BALANCING PUBLIC INTEREST AND PRIVATE RIGHTS

Although the public may have some interest in obtaining access to information produced in litigation, litigants themselves have important rights that are protected under the Constitution—rights that may be lost if information subject to a protective order to settlement agreement is disclosed. Both the public's interest in access and litigants' interest in privacy cannot be satisfied; they are mutually exclusive. Allowing public access to information whose value depends on its confidentiality destroys the property or privacy right in the information. Denying public access to confidential proprietary information protects the property or privacy right but disregards the public's interest. Resolution of this conflict requires a choice between the two competing interests.

Logic and fundamental fairness dictate a presumptive choice in favor of the litigant. Before a lawsuit is filed, the public has no right of access to confidential information kept by a private individual or organization. Nothing dictates that the mere filing of a lawsuit changes this fact and creates a right of public access to the information that did not previously exist. On the other hand, the future litigants have a plethora of legal rights and interests, including their rights in confidential information.

When a lawsuit is filed, a specific subset of the litigants' rights or interests is placed in question—that is, the legal issue to be decided in the lawsuit. The litigants' remaining rights and interests that are not at issue in the lawsuit, including the rights they have in confidential information, should remain just the same during and after the lawsuit as they were prior to the lawsuit.

---

38. Nixon v. Adm'r Gen. Servs. Admin., 433 U.S. 425, 431 (1877), *aff'g* 408 F.Supp. 321 (D. D.C. 1976).

39. Whalen v. Roe, 429 U.S. 589, 605-07 (1977), *rev'g* 463 F.Supp. 931 (S.D. N.Y. 1975).

40. Wisconsin v. Constantineau, 400 U.S. 433, 435 (1971), *aff'g* 302 F.Supp. 861 (E.D. Wis. 1969).

41. Old Dominion Dairy Products v. Sec'y of Defense, 631 F.2d 953, 963 (D.C. Cir. 1980).

42. Codd v. Velger, 429 U.S. 624 (1977).

43. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989), *rev'g* 816 F.2d 730 and 831 F.2d 1124 (D.C. Cir. 1981); Utz v. Cullinane, 520 F.2d 467, 476 (D.C. Cir. 1975); Tarlton v. Saxbe, 507 F.2d 1116, 1124 n.23 (D.C. Cir. 1974).

For example, a plaintiff may be required to produce intensely private medical records in order to resolve a personal injury action. The information is needed as a tool to resolve the underlying issues of liability and the plaintiff's right to recover compensation. The information itself and the plaintiff's right to keep it confidential, however, are not the underlying legal issues. Although requiring production of this information is fair in order to resolve the lawsuit, going one step further and allowing public access to the medical records, thereby destroying the privacy right in them, is not fair.

The same holds true for a defendant required to produce design information in order to vindicate itself in a product liability case. Any property right the defendant had in the information before the litigation should not be destroyed because of public disclosure through the litigation.

The law should and does authorize courts to ensure a sort of legal homeostasis for rights and legal interests that are unavoidably brought into court along with the actual legal issues that are central to resolving the dispute. Without this protection, citizens would be reluctant to use the court system because vindication of one legal right might result in the loss of other, perhaps more important, rights. Litigants have a compelling argument that their interests in confidentiality should override the public's interest in access, particularly when those rights rise to the level of property or privacy rights protected under the Constitution. The serendipitous or perhaps even the malicious filing of a lawsuit are not legitimate grounds for allowing the invasion of the litigants' property and privacy rights.

MEDIA HYPE, PLAINTIFFS BAR FRENZY ARE JUST THAT

None of the media hype or the frantic pleas from the organized plaintiffs' bar can change the reality of the law or the facts. The law protects confidential information produced in litigation but not used in judicial proceedings. Nothing has been proposed or exposed that warrants a change in this fundamental tradition of American jurisprudence. Courts that act or find to the contrary are at risk of being like the emperor duped by the outrageous claims of the clever tailors—they may be emperors with no clothes.

The Privacy Project

The Brave New World Is Here: Privacy Issues and the Human Genome Project

Governments and courts must step in to provide protections and regulations for the use of individuals' genetic testing results

By Robert A. Curley Jr. and Lisa M. Caperna

SCIENTIFIC discoveries and advances in biological understanding during the 20th century paved the path for the Human Genome Project.

"We used to think our fate was in our stars. Now we know, in large measure, our fate is in our genes," said James Watson, who co-discovered the double-helix structure of DNA with Francis Crick in 1953.[1] As for Crick's thoughts, he stated, "You, your joys and your sorrows, your memories and your ambitions, your sense of personal identity and free will, are in fact no more than the genetically determined behavior of a vast assembly of nerve cells and their associated molecules."[2]

DNA was discovered in the mid 1800s. In 1868, a Swiss biologist, Friedrich Miescher, identified DNA in the nuclei of pus cells obtained from discarded surgical bandages. But it was during the 20th century that there were great advances in biological understanding of DNA.

In 1943, American Oswald Avery proved that DNA carries genetic information. He even suggested that DNA might actually be the gene. Most people at that time thought the gene would be protein, not nuclei acid, but by the late 1940s, DNA generally was accepted as the genetic molecule. In 1952, Alfred Hershey and Martha Chase performed the definitive experiment that showed that DNA was, in fact, the genetic material.

Once more was known about DNA, the next step was to figure out the molecule's structure. The race was on. At Cambridge University, there were Watson and Crick. At the same time, at King's College in London, Maurice Wilkins and Rosalind Franklin also were studying DNA. In 1953, building from the King's team's research, Watson and Crick presented a model of the structure of DNA. In 1962, Watson, Crick and Wilkins shared the Noble Prize for physiology and medicine. Franklin had died by 1962, and the Nobel Prize rules do not allow an award to be made posthumously, and interestingly nor do they allow more than three scientists to share the award.

Franklin actually was the one who discovered and first stated that the sugar-phosphate backbone of DNA lies on the outside of the molecule. She arrived at this discovery after examining the DNA molecule under an x-ray beam, a technique called x-ray crystallography. It would be

IADC member Robert A. Curley Jr. is president of Curley & Curley, P.C., of Boston, where he concentrates his practice in the defense of product liability and catastrophic personal injuries. He is a graduate of Harvard College (A.B. 1971) and Cornell University Law School (J.D. 1976).

Lisa M. Caperna is an associate at Curley & Curley. She was educated at Boston College (B.A. 1997, J.D. 2000).

1. James Watson, quoted in Leon Jaroff, *The Great Hunt*, TIME, March 20, 1989, at 62, 67.

2. FRANCIS CRICK, THE ASTONISHING HYPOTHESIS: THE SCIENTIFIC SEARCH FOR THE SOUL 3 (1994).

interesting to know which three of the four scientists would have received the Nobel Prize had Franklin not died before the award was given.

Although genetics dates back to the mid 1800s, the last decade has proved to offer the milestones in genetic history, what with technology advances and revolutionary scientific endeavors like the Human Genome Project. DNA's discovery has been called the most important biological work of the last hundred years, and the research that it has sparked will lead to monumental developments in the next hundred.

HUMAN GENOME PROJECT

A. What Is It?

The Human Genome Project (HGP) is an international research effort to determine the sequence of the three billion chemical base pairs that make up the human DNA and to identify the approximately 35,000 genes in human DNA. While the HGP was conceived as early as the mid 1980s by scientists in the U.S. Department of Energy, the initial planning process culminated in 1990. Since then, researchers from the United States, the United Kingdom, Germany, Japan, China and France have been reconstructing DNA sequences to produce detailed physical maps of the human genome.

The international consortium is supported mostly by the U.S. National Institutes of Health and the Wellcome Trust, a philanthropic organization based in London and directed by Dr. Michael Dexter. Other governmental agencies and charitable institutions in the various countries also fund the project. The driving force behind the project is the identification and eradication of all genetically based diseases.

The U.S. Human Genome Project is a 13-year effort coordinated by the Department of Energy and the National Institutes of Health. The project originally was planned to last 15 years, but effective resource and technological advances have accelerated the expected completion date to 2003. Francis Collins, the director of the project at the National Institutes of Health, has said, "It's hard to overstate the importance of reading our own instruction book, and that's what the Human Genome Project is all about."[3]

The United States also is home to the prominent private endeavor to map the human genome being done by Celera Genomics, a company in Rockville, Maryland, headed by J. Craig Venter.

B. Basic Science

For a better understanding of the work being done by the HGP, it may be useful to review Biology 101. Every human cell (except for red blood cells and the platelets that are critical to normal blood clotting and wound healing) contains a nucleus that has within it roughly six feet of a special chemical called deoxyribonucleic acid, or DNA. DNA consists of a backbone of repeating sugar and phosphate units, each of which binds a simple chemical structure called a nucleotide (more commonly, a "base"). There are four kinds of bases found in DNA, and these are abbreviated: A for adenine, C for cytosine, G for guanine, and T for thymine.

There are 46 strands of DNA in each human cell, and they coil into the condensed double helix shape contained in 23 pairs of chromosomes. The 46 molecules of DNA contain an estimated 35,000 genes. Each nucleus-containing cell in an individual's body has the same DNA. There are three billion DNA bases in a cell, called the genome. Technically, there are six billion base pairs of DNA; at conception, three billion bases in an unfertilized egg are joined with three billion from the male sperm. Scientists think the two sets differ by about one DNA base in every one thousand, differences that can be explored after one set has been sequenced.

Encoded within the structure of the nucleotide DNA chain is the information necessary for cell structure and function. The DNA strand includes coding regions, called genes. The sequence of nucleotide sub-units in genes directs cells to produce proteins, which provide structure to and

mediate chemical reactions within a cell. Thus, proteins determine the characteristics of cells, which in turn collectively determine the characteristics of the individual. There are an estimated 35,000 genes in the human genome.

It is interesting to note that the remaining DNA, which may exceed 95 percent of the total and is unknown at this time, does not code for proteins and is often referred to as "junk" DNA. Further scientific exploration is necessary to determine the function of this DNA.

Genetic disorders may occur when there is a mutated gene. Sometimes full segments of DNA may be missing, multiplied or transposed—that is, found on a different segment of the chromosome. A classic unusual example of a mutation-based genetic disease is sickle-cell anemia, in which precisely one A (the nucleotide, or base, adenine) has been replaced by a T. These mutations may be either inherited or acquired. Such mutations may then lead to genetic disease.

Genetic disorders may be classified as either "multi-factorial" or "single-gene" genetic conditions.[4] Multi-factorial conditions may not manifest themselves in the absence of certain behavioral or environmental factors. These conditions rely on the interaction of numerous genetic and environmental factors. In the case of single-gene diseases, such as cystic fibrosis and Huntington's disease, the carrier received a gene in which the disease will manifest itself regardless of environmental factors.

It is important to distinguish between the terms "predisposed genetic condition" and "pre-symptomatic genetic condition." People who are predisposed to a genetic disease do not have the disease. Rather, they have an increased likelihood that the disease will develop. On the other hand, people with pre-symptomatic genetic conditions will develop the disease if they live long enough. An example of such a condition is Huntington's disease.

Another aspect of genetic diseases is the gene's penetrance and expressivity. Penetrance is the likelihood that a gene will express itself. For example, the BRCA1 gene, which predisposes an individual to breast cancer, is about 85 percent penetrant, while the Huntington's gene is 100 percent. Expressivity deals with the severity and manner in which the gene manifests itself once it has penetrated. For instance, two women with the BRCA1 gene may develop breast cancer at different ages and in varying degrees of severity. It is important to remember that not everyone who develops breast cancer has the BRCA1 gene; some may have "acquired" this genetic disease because of mutations that may form spontaneously from environmental factors, such as radiation, or age-related factors. The BRCA1 gene is responsible for approximately 5-10 percent of breast cancer, while 90-95 percent of breast cancers are spontaneous genetic disorders.[5]

Wondering if you missed a day of Biology 101? Rest assured, whatever you missed, you will learn as the Human Genome Project's discoveries continue to make headlines. With the project's growing popularity, good or bad, it is likely that what may not have been part of the curriculum of the past, will be common knowledge in the future.

C. HGP's Goals

The ultimate goals of the Human Genome Project are to identify the approximately 35,000 genes in human DNA and to map out and sequence the three billion chemical base pairs that make up human DNA.[6] In other words, to produce the human blueprint.

Mapping is a process that results in knowing the location of the gene on a chain of DNA. Sequencing is breaking

---

3. *See* "Rough Map of Human Genome Project Completed" at www.cnn.com/2000/health/06/26/human.genome.03/index.html (visited June 26, 2002).

4. *See* Christopher M. Keefer, *Bridging the Gap Between Life Insurer and Consumer in the Genetic Testing Era: The RF Proposal*, 74 IND. L.J. 1375, 1378 (Fall 1999).

5. *Id.*

6. *See* Human Genome Project Information at www.ornl.gov/hgmis (visited May 30, 2002).

down the biochemical parts of the DNA that composes each gene into its nucleotides. The DNA sequence refers to the order of the nucleotides (A, C, G, and T) in the DNA chain.

The scientific techniques used by the Human Genome Project to detect altered genes result in the mapping of genetic diseases. Once a section of an individual's DNA is mapped, it can be compared to known sequences created by the project to determine whether the individual has the specific gene or genes that causes a genetic condition or makes the individual more susceptible to a genetic condition.

The genes that are mapped and sequenced in the project do not come from one human being but from cell lines that have been acquired and grown in many laboratories over a long period of time. These blueprints are then compared to maps of individuals with genetic disorders in order to track down components of a genetic disorder. Finding all of the components of a complex genetic disorder requires analyzing entire genomes of hundreds and, in some cases, thousands of individuals.

Although called the Human Genome Project, the project involves sequencing the DNA of many other organisms, such as the mouse, rat, worm, fly and yeast. The theory behind this is that the human genome should not be studied in a vacuum. Learning how the human genome compares to those of other organisms will help an understanding the human genome's makeup and how it has evolved.

Additional goals of the U.S. Human Genome Project include storing this information in databases, improving tools for data analysis, transferring related technologies to the private sector, training scientists who will be able to utilize the tools and resources developed to pursue biological studies that will improve human health, and examining the ethical, legal and social implications of human genetics research. In an effort to achieve some of these goals, the project has licensed technologies to private companies and awarded grants for innovative research.

D. Progress to Date

In June 2000, President Clinton announced the completion of a "working draft" of the human genome, a collection representing more than 90 percent of the genetic composition of chromosomes. Approximately 75 percent of the sequence is in a highly accurate "finished" state. The other 25 percent is merely "draft" quality. This accomplishment led to the February 12, 2001, declaration of the first readable draft of the "Book of Life."[7]

While there are still some gaps to be filled, scientists are already forming a good idea of what the genome looks like. First**,** it turns out that human chromosomes have crowded centers with many genes in close proximity to one another and vast expanses of unpopulated areas where only non-coding "junk" DNA are found.[8] This distribution of genes is very different from the genomes of the other organisms sequenced by the HGP. The other organisms studied have genes that are relatively evenly spaced throughout.

Scientists also learned that human beings have only about twice as many genes as the worm or fly. Apparently, humans are able to do more with what they have than other species. Instead of producing only one protein per gene, the average human gene produces three different proteins.

Moreover, the HGP has made significant progress in discovering the links between human genes and diseases. For instance, scientists have identified the genes for cystic fibrosis, Tay Sachs disease, sickle cell anemia, Duchenne muscular dystrophy, hemophilia A, Alzheimer's disease, Huntington's disease and various forms of cancer.

---

7. *See* Human Genome Project Information, "The Science Behind the Human Genome Project," at www.ornl.gov/hgmis/project/info.html (visited August 23, 2002).

8. *See* National Genome Research Institute, "International Human Genome Sequencing Consortium Publishes Sequence an Analysis of the Human Genome," at www.nhgri.nih.gov/news/initial_sequence PR.html (visited May 1, 2002)

E. Likely Future Developments

While scientists have identified a significant number of genes and have linked many of them to known single-gene diseases, there are thousands of genes yet to be understood, or even identified for that matter. It may take years or even decades to identify genes that do not have the typical sequence characteristics of a gene.

Moreover, although geneticists have pinpointed the genetic mutations behind some single-gene diseases, there are still multigene diseases that will be far more complicated to identify. Because each errant gene makes only a small contribution to such diseases, it has no obvious pattern of inheritance and its presence is hard to find among the natural variations in DNA sequence.

It also is important to keep in mind that the draft of the "Book of Life" may have some inaccuracies. In fact, a private company in Iceland, called Decode Genetics, already has found some mistakes. Decode was founded by Dr. Kari Stefansson, a former Harvard neuropathologist, who chose Iceland because of its small population (278,000) and careful genealogic record keeping, which allows disease genes to be traced back more than 10 generations. Through its detailed knowledge of Icelandic genomes, Decode has uncovered and has been able to correct many errors in the human genome sequence produced by the HGP. For example, Decode discovered that in more than 100 cases, large sections of the consortium's human genome are in the wrong order or flipped head-to-tail, and the wrong order degrades the statistical power of gene-hunting methods.[9]

In the near future, there likely will be improvements to the draft sequence, along with the identification of single-gene and a few multi-gene diseases. In the meanwhile, continuous findings of the Human Genome Project will affect aspects of clinical medicine far beyond what is currently thought of as genetic disease. As technology for molecular testing improves and turnaround time for test results decreases, current common diagnostic tests will be supplanted by nucleic acid-based analyses. Gene therapy, through which the errant gene is replaced with a normal gene, may become a common and practical way to treat genetic diseases.

As for the next group of genomes to be sequenced, the National Human Genome Research Institute has announced its "dream team." The organisms designated as high priority for sequencing include chickens, chimpanzee, several species of fungi, sea urchins and honey bees.[10]

EXPECTATIONS OF PRIVACY

A. What is Privacy?

Dictionary definitions of "private" and "privacy" include "belonging to oneself," "intended for or restricted to the use of a particular person or group," "not freely available to the public" and "freedom from unauthorized oversight or observation." In the context of human genetic material, these definitions involve fundamental concepts of ownership ("belonging") and, more important, authorized use.

B. Traditional Property Concepts

Generally speaking, a person has property rights in his or her body, although there has been some legal reluctance in terming the human body as property. The Uniform Anatomical Gift Act, which has been widely adopted in the United States, authorizes competent adults to make gifts of all or any part of their body to take effect on death.[11] The act limits donees to medical or dental care providers and schools, banks or storage facilities for medical or dental education, research, ad-

---

9. *See* Nicolas Wade, *Hunting for Disease Genes in Iceland's Genealogies* [www.nytimes.com/2002/06/18/health/genetics/18prof.html] and *A Genomic Treasure Hunt May Be Striking Gold* [www.nytimes. com/2002/06/18/science/18deco.html], both June 18, 2002.

10. *See* National Genome Research Institute, "NHGRI Prioritizes Next Organisms to Sequence," at www.nhgri.nih.gov/NEWS/news.html (visited May 30, 2002)

11. The text of the act, together with the prefatory note and comments, are available at www.law.upenn.edu/bll/ulc/fnact99/uaga87.pdf.

vancement of medical or dental science, therapy or transplantation or any specified individual for medical therapy or transplantation. It authorizes gifts by living donors for transplantation where the donor and two physicians who examined the donor and who are involved in the transportation sign an affidavit.

A person's heirs have certain property rights in the deceased person's body and organs. As one court observed, in a case involving unauthorized cornea removal, "property is often conceptualized as a 'bundle of rights' . . . which . . . include the right to possess, to use, to exclude, to profit, and to dispose."[12]

Blood may be donated, but that act and the blood's use is subject to substantial governmental regulation.[13]

Persons unquestionably have property rights in their own DNA, but those rights may be subject to greater societal and governmental interests. The Supreme Court of Indiana has ruled that a rape suspect "had a legitimate expectation of privacy in his body and blood samples" when they were taken in a rape prosecution for which he was acquitted on the basis of a consent defense. In a later prosecution for another rape, the court held that once his DNA, which was collected pursuant to statute, became part of the DNA bank, "the profile becomes the property of the crime lab." The defendant had no expectation of privacy in the sample in the database, the court ruled, and that there had been no violation of the Fourth Amendment.[14]

In 1993, the United States enacted legislation (42 U.S.C. § 14132 *et seq*.) mandating the creation of an index of DNA identification records of persons convicted of crimes and analyses of DNA from crime scenes, unidentified human remains and (by later amendment) missing persons. The states followed suit.[15]

The original federal legislation addressed privacy rights by limiting disclosure of stored DNA information to criminal justice agencies, to courts in judicial proceedings where DNA evidence is admissible, and to criminal defendants for defense purposes. Disclosure also was limited for a population statistics database, identification research and protocol development, or for quality control, but only if personally identifiable information was removed. Violation of the privacy provisions was made a crime punishable by a fine of up to $100,000.

In 2000, a specific privacy protection section was added (42 U.S.C. § 14135(e)), and the Federal Bureau of Investigation and states accessing the index were required to expunge the DNA records of persons whose criminal convictions were overturned (42 U.S.C. § 14135(d)).

C. Abandoned Property

Human beings constantly shed samples of their DNA into the environment—hair, saliva, blood. Does an individual have a property right with respect to DNA no longer directly attached to their person? In the context of DNA found at crime scenes, the answer clearly is no.

In a case involving impressions of counterfeit bills in sealed trash bags left on a sidewalk, the First Circuit held that the defendant had no expectation of privacy as to the content of the bags,[16] but there is contrary authority.[17] Absent legislation, the American rule is that title to abandoned property rests in the finder.[18]

In the brave new world of DNA technology, where it is probable that samples of DNA can be extracted from any trash bag left on the sidewalk—for example, saliva on an envelope—the law may need to address previously unthought-of privacy concerns. In criminal cases, the interest of the government probably will trump any argu-

---

12. Whaley v. County of Tuscola, 58 F.3d 1111, 1114 (6th Cir. 1995), *cert. denied*, 516 U.S. 975 (1995).
13. *See, e.g.*, MASS. GEN. LAWS ch. 111, §§ 184(B); 105 MASS. REGS. CODE § 135.001 et seq
14. Smith v. Indiana, 744 N.E.2d 437 (Ind. 2001).
15. *See, e.g.*, MASS. GEN. LAWS ch. 22E, § 1 et seq.
16. United States v. Mustone, 469 F.2d 970 (1st Cir. 1972).
17. California v. Krivda, 486 P.2d 1262 (Cal. 1971), *vacated and remanded*, 409 U.S. 33 (1972).
18. Massachusetts v. Maritime Underwater Surveyors Inc., 531 N.E.2d 549 (1988).

able privacy expectations. But in situations involving the collection, analysis or use of abandoned DNA by non-governmental persons or entities in non-criminal and commercial situations, a different balance may be in order.

D. Traditional Tort Concepts

Section 652A of the Restatement (Second) of Torts recognizes an invasion of a right to privacy by an unreasonable intrusion on the seclusion of another, by the appropriation of another's name or likeness, by unreasonable publicity given to the other's private life, or publicity that unreasonably places the other in a false light. The commentary indicates that an invasion of privacy is actionable where it would be highly offensive to a reasonable person. According to Section 652H of the Restatement, damages recoverable for an invasion of privacy include damages for the harm to the interest in privacy, mental distress and special damages. In this era, most people would probably find any unauthorized location, extraction and use of their DNA to be highly offensive.

In the absence of any statutory framework for civil actions arising from the location, extraction and use of DNA, tort law will be the arena in which the parameters of privacy rights in DNA will develop.

E. Authorized Extraction and Use of Genetic Data

1. Non-consensual DNA Testing

In the context of criminal prosecution, the taking of a blood sample may be non-consensual, provided there is probable cause and a search warrant or exigent circumstances justifying the lack of a warrant.[19] Compulsory provision of blood for the purpose of blood typing and DNA analysis in the course of a criminal prosecution may be authorized, subject to constitutional limitations.[20]

All U.S. states have enacted legislation providing for databases of DNA from certain convicted criminals.[21] The use of reasonable force to collect DNA samples is authorized under these laws.[22] These statutes have been held constitutional in view of the low expectation of privacy of convicted criminals, the governmental need for a reliable system of identification of convicted criminals and the minimal intrusion involved in a pin-prick.[23] As with the federal DNA database in the United States, privacy rights have been addressed by restricting the authorized use of the database and creating criminal penalties.[24]

Legislation has authorized courts to order genetic marker testing in paternity actions. Privacy issues are addressed by closing trials to the public and segregating records. An adverse inference may be drawn from a refusal of any party to submit to a genetic marker test.[25]

2. Consensual DNA Testing for Research

Biotechnology and companies with "gen" in their names are hot. Academic kudos will be heaped on those who continue to unlock the secrets of the human genome. Research requires the acquisition of genetic material, especially where groups of individuals with a specific characteristic are the subject of study.

Consent may take many forms, as it is essentially a private agreement. With respect to university-sponsored or private research, consent may be subject to compliance with university or company guidelines on research.

Consensual donation of genetic matter for the purposes of research either for the acquisition of pure knowledge or commercial application raises numerous issues.

From the viewpoint of personal privacy,

---

19. Schmerber v. California, 384 U.S. 757, 767 (1966).
20. United States v. Goodridge, 945 F.Supp. 371 (D. Mass. 1996).
21. *See* Laudry v. Attorney General, 709 N.E.2d 1085, 1087 (Mass. 1999).
22. *E.g.*, MASS. GEN. LAWS ch. 22E, § 4.
23. Laudry, 709 N.E.2d 1085.
24. *E.g.*, MASS. GEN. LAWS ch. 22E §§ 9-14.
25. E.g., MASS. GEN. LAWS ch. 209C, §§ 11, 12-13, 17.

it would be desirable for genetic samples used in research to be identified in a way that does not involve the name of the donor—for instance, by an alphanumeric designation—and which would prevent the research team from immediate knowledge of the identity of the person whose genetic material is the subject of research. While it is conceptually possible to devise a manner of purely anonymous donation of genetic material, such a system is probably less desirable from a number of viewpoints than one in which the material can be traced to a specific donor. From the viewpoint of research, it may be desirable to obtain additional follow-up data from the donor. From the viewpoint of the donor, it may be desirable to know the results of the genetic testing. Existing systems for the protection of the privacy of medical test data could probably serve as the model for privacy protection in this area.

In obtaining consent for the testing of genetic material, it probably is prudent to address one of the thorniest ethical issues in this area: Should the donor be informed of the results if they disclose the possibility, probability or certainty that the donor will develop certain medical conditions—for example, Huntington's disease—or has a genetic trait that may have an arguably adverse effect on offspring? In some cases, these disclosures could have an adverse effect on the donor's life long before the actual development of a medical condition. At the time of consenting to genetic testing, the donor probably should be informed, within reason, of the possible results of genetic testing, and the donor's informed choices should be honored.

Consent for research involving donated genetic material probably should address, at least generically, the use of the research and any connected commercial application. Donors should know that they are surrendering any property right in their genetic material, subject to privacy protections, and that they have no right to prevent or control the appropriate publication of the research results or the commercial application of the knowledge derived from the research.

3. Present Protection

It is a "brave new world," a world in which an individual's strand of hair or speck of dandruff can be tested for the presence of a myriad of genetic conditions and diseases. As advances in technology make it easier to access and understand the mysteries of the human genetic code, the potential of abuse of such information becomes a real threat. Putting aside the fear of human cloning and designing the "perfect" child, there is a growing concern that dissemination of an individual's genetic information will result in discrimination by employers and insurers. The primary concerns are that insurers will use genetic information to deny, limit or cancel insurance policies and that employers will use the information against their workers or to screen potential employees. The main question is: Do current laws protect people from this abuse? The answer: Maybe.

a. Federal Law

At the federal level in the United States, the only legislation enacted to date that directly prohibits genetic discrimination is the Health Insurance Portability and Accountability Act of 1996, known as HIPAA (Pub. L. No.104-191). HIPAA states that genetic information shall not be considered a pre-existing condition in the absence of a diagnosis of the actual condition. The protection afforded by the HIPAA is limited, however, as it does not prohibit rate increases as a consequence of genetic test results, it does not cover individuals who are not in a group plan, and it does not protect against discrimination by employers.

There are several federal statutes that may offer some protection against genetic discrimination in the workplace. For instance, Title VII of the Civil Rights Act of 1964 (42 U.S.C. § 2000e *et seq*.) may protect individuals to a limited extent. Under Title VII, employers are prohibited from discriminating on the basis of sex, race, national origin, religion or color. Since a few genetic diseases are tied strongly to sex, race or ethnicity, an employer that discriminates against an employee based on

such genetic diseases may violate Title VII. For example, in *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*,[26] the plaintiffs, without their consent, were subjected to pre-employment screening that included sickle-cell testing for African Americans. The plaintiffs prevailed. However, most genetic conditions are not predominately linked to a certain sex, race or ethnicity.

For broader protection, one might be tempted to turn to Title I of the Americans with Disabilities Act of 1990 (ADA), enforced by the Equal Employment Opportunity Commission (EEOC) for protection against genetic discrimination in the workplace, and similar disability-based anti-discrimination laws, such as the Rehabilitation Act of 1973. 42 U.S.C. § 12101 *et seq*.; 29 U.S.C. § 701(b)(1)-(2). While these laws do not explicitly address genetic information, they provide some protections against disability-related genetic discrimination in the workplace. The ADA, however, applies only to employers with 15 or more employees.

Under the ADA, a person with a disability is defined as one who either (1) has a physical or mental impairment that substantially limits a major life activity, (2) has a record of such impairment or (3) is regarded as having such an impairment. The ADA would seem to cover people who have a manifested genetically related illness or disability that impairs a major life activity, as well as those who have a record of a genetically related disability. But does it prohibit discrimination based on a diagnosed asymptomatic genetic condition that does not substantially limit a major life activity? In 1995, the EEOC adopted the view that discrimination on the basis of genetic information is covered under the third prong of the ADA's definitions of "disability."[27] A recent U.S. Supreme Court case, however, suggests otherwise.

In *Bradgon v. Abbott*,[28] the Court held that a person with asymptomatic HIV is a covered individual with a disability under the ADA. The Court found a physical impairment based on cellular and molecular changes that take place in the body as a result of the infection. Although similar reasoning might support the argument that the ADA covers individuals with asymptomatic genetic predisposition under the first prong of the ADA's definitions, Chief Justice Rehnquist's dissenting opinion suggests that the justices might be reluctant to define individuals with genetic alterations as disabled within the meaning of the ADA. The justices reasoned that the possible effect of finding such individuals disabled would be that all individuals with genetic alterations would be considered disabled and, consequently, protected under the ADA. Given that, according to scientists, every person has genetic alterations of some form, it does make sense to draw the line somewhere.

While the ADA does not specifically address genetic testing, it discusses medical examinations and inquiries. It divides medical examination and inquiries into three stages: pre-employment, pre-placement and post-placement. At the pre-employment stage, the employer is prohibited from asking prospective employees if they are disabled and cannot conduct a medical examination. The employer, however, can make offers of employment contingent on the successful completion of a pre-placement medical examination. At the pre-placement stage, the employer is allowed to administer a medical examination as long as all entering employees are tested and the information is kept confidential, with only a few exceptions. Similarly, the employer may require the release of all of the individual's medical records. Post-placement, an employer can require employees to undergo a medical examination if the examination is job-related and consistent with business necessity.

---

26. 135 F.3d 1260, 1264 (9th Cir. 1998).

27. Human Genome News, "Analyzing Genetic Discrimination in the Workplace," remarks of EEOC Commissioner Paul Miller at the EINSHAC International Working Conversation on Enviro/Genetic Disputes and Issues, July 2001, available at www.ornl.gov/hgmis/publicat/hgn/v12n1/09workplace.html (visited May 9, 2002).

28. 524 U.S. 624, 657-62 (1998), *vacating and remanding* 107 F.3d 934 (1st Cir. 1997). Decision below, 912 F.Supp. 580 (D. Me. 1995).

It is important to note that there are no limits placed on pre-placement tests, and an individual who undergoes the tests has no right to be told what tests are being conducted, the test results, or how the information generated by the tests will be used in determining employability. Moreover, if the employer decides to withdraw a conditional offer of employment, the individual has no right to be told why, not even that the withdrawal was based on the test results. Although the ADA prohibits the withdrawal of a conditional offer for medical reasons, unless they are job-related, individuals usually will not know the reason unless they pursue a legal action against the employer.

The permissible scope of an employee's medical examination raises significant concerns about genetic privacy. Individuals may be reluctant to undergo genetic testing, even if they are at risk for some genetic condition or disease, because they fear that their employer, on whom they may depend for health insurance, will access their medical records. Individuals may also be worried that any time they have a blood test, their employer could perform genetic testing without obtaining consent or informing the employee.

In the near future, an employee's genetic privacy may be in jeopardy even if the employee does not have an exam. Imagine what once was possible only in science fiction thrillers. Unscrupulous Manager sneaks into Associate's office after hours to confiscate Associate's coffee mug. The next morning, Manager sends mug to company's lab to have Associate's remnant saliva genetically tested. That afternoon, Manager fires Associate because he's predisposed to lung cancer and he's on the company health insurance plan.

If you think this is too easy, think again. By 2010, scientists predict that the modest sum of $100 will buy a test that effectively identifies genetic markers for a myriad of conditions and diseases.[29]

Perhaps genetic discrimination is too different from traditional disability discrimination for the ADA or other disability-based anti-discrimination statutes to be adequate protection against it. Even where genetic discrimination may reasonably fall under the purview of the ADA, courts may find that it does not. Legislation introduced in the U.S. Congress last session by Senators Thomas Daschle and Edward Kennedy would prohibit discrimination by private sector employers on the basis of genetic information and provide strong privacy protections to any genetic information used for medical treatment and research.

The Daschle-Kennedy bill was based on a presidential executive order of February 8, 2000, which prohibits federal employers from considering genetic information in hiring, promoting, discharging and all other employment decisions.[30] Under the executive order, obtaining or disclosing genetic information about employees or potential employees is prohibited, except where it is necessary to provide medical treatment to employees, ensure workplace health and safety or provide occupational and health researchers access to data. Under these exceptions, genetic monitoring is allowed. Genetic monitoring determines to what degree a person has been exposed to or harmed by toxins in the work environment. As an executive order and not legislation, it applies only to former and present employees and applicants for employment by the federal government.

With respect to protecting against the unlawful dissemination of genetic information, Congress' best effort thus far is the recently enacted HIPPA National Standards to Protect Patients' Personal Medical Records. This new regulation protects medical records and other personal health information maintained by health care providers, hospitals, health plans and health insurers, and health care clearinghouses.

The new standards limit the non-consensual use and release of private health information; give patients new rights to access

---

29. Human Genome News, *supra* note 27.

30. Exec. Order No. 13,145 (February 8, 2000), 3 C.F.R. 13,145. *See* Human Genome Project Information, "Genetics Privacy and Legislation," available at http://www.ornl.gov/hgmis/elsi/legislat.html (visited May 1, 2002)

their medical records and to know who else has accessed them; restrict most disclosure of health information to the minimum needed for the intended purpose; establish new criminal and civil sanctions for improper use or disclosure; and establish new requirements for access to records by researchers and others.[31] Note, however, that these standards are not specific to genetics.

b. State Law

Currently, about half the states have legislation prohibiting genetic discrimination in the workplace. State legislatures began enacting such laws in the 1970s as a response to discrimination against individuals carrying the sickle cell trait. Since that time, most states have updated their laws to varying degrees.

Some states have broad bans on discrimination while others specify particular types of discrimination that are prohibited. Rhode Island, New Hampshire, Texas and Oklahoma are among the states that broadly prohibit discrimination based on genetic information and provide no exceptions.[32] In contrast, other states, including Delaware, Maine, Michigan, Arizona and Massachusetts, allow employers to consider and in some cases collect genetic information, if it can be proved to be job related and consistent with business activity.[33] Then there are states like Illinois with legislation stating that "an employer shall treat genetic testing information in such a matter that is consistent with the requirements of federal law, including but not limited to the ADA."[34]

While it is reassuring to see so many states explicitly addressing genetic discrimination, the legislation has generated many questions. For examples: What is meant by a genetic test? Is genetic information distinct from or merely one form of medical information? Should a tissue sample and data derived from it be the property of the person from which it was taken?

Definitions of a genetic test vary widely. Some states define it as "a test of an individual's DNA, RNA, or chromosomes . . . associated with a predisposition for a clinically recognized disease or disorder." Because this type of definition does not include the testing of proteins, it excludes some newborn screening, prenatal tests for neural tube defects, along with many tests currently used to make diagnoses. Other states are more inclusive in that they define genetic testing as analysis of a chromosome, a gene, DNA, RNA, or protein encoded by a gene.

Whether genetic information is so different from other clinical data that it deserves special protection is another issue that must be addressed when legislation is drafted. Considering that genetic tests may predict future risks for a healthy individual and may imply risks about that individual's relatives, such data seems to warrant more

---

31. For a fuller discussion of the HIPPA regulations, *see* Nancy A. Lawson, Jennifer M. Orr & Doedy Sheehan Klar, *The HIPAA Privacy Rule: An Overview*, in this issue of *Defense Counsel Journal*, page —.

32. R.I. GEN. LAWS § 28-6.7-1; N.H. REV. STAT. ANN. § 141-H:3; TEX. LAB. CODE ANN. § 21.402; OKLA. STAT. tit. 36, § 3614.2.

33. DEL. CODE ANN. tit. 19, § 711 prohibits an employer from discriminating against an individual based on genetic information and from intentionally collecting any genetic information concerning an employee or an applicant for employment, or any member of their family, unless it can be demonstrated that the information is job related and consistent with business necessity or the information is sought in connection with the a benefit plan.

ME. REV. STAT. ANN. tit. 5, § 19302 prohibits an employer from discriminating against an individual based on genetic information, except when based on a bona fide occupational qualification.

MICH. COMP. LAWS § 37.1202 prohibits an employer from refusing to hire, recruit, or promote an individual based on genetic information unrelated to the individual's ability to perform the duties of the job; from requiring an individual to submit to a genetic test or to provide genetic information; and from acquiring or accessing genetic information concerning an employee, an applicant for employment or a member of the employee's or applicant's family.

ARIZ. REV. STAT. § 41-1463 prohibits an employer from discriminating against an individual based on genetic information, but allows an employer to give and act on the results of any professionally developed ability test.

MASS. GEN. LAWS ch. 151B, § 4 prohibits discrimination because of genetic information unless based on a bona fide occupational qualification).

34. 410 ILL. COMP. STAT. 513/25 (2001).

protection than other medical information. On the other hand, separating genetic information from other medical information may not be easy.

As genetic testing becomes part and parcel of common medical care, it will be difficult to enact draft legislation that requires separate treatment of portions of patients' medical records. One solution may be language that covers the access to and use of all medical information. Arizona is on the right track with a statute that provides broad protection to genetic privacy based on confidentiality rather than specifying situations in which genetic discrimination is prohibited.[35]

Whether tissue samples and the genetic data derived from them should remain the property of the individual tested also is an issue that has stirred debate. In 1996, Oregon enacted legislation specifically providing that an individual's genetic information is the property of the individual.[36] In 1996, the New Jersey legislation passed a similar bill, but it was vetoed by then-Governor Whitman because of protests from the pharmaceutical industry. Researchers seem to want a clear right to use samples. A later version of the bill, which the governor did sign, excluded the property provision but required that genetic testing be preceded by written informed consent.[37]

In 2002, a third New Jersey bill, providing that an individual's genetic information is the property of the individual, passed.[38] This most recent enactment also amended the 1996 legislation by applying the former's provisions concerning notification of genetic test results to the person who performs the test—that is, a clinical laboratory—rather than a person who requires or requests that genetic testing be done—that is, an insurance carrier.

NASCENT GENETIC ISSUES

A. Regulation

While the states serve as legislative laboratories in the United States, the need for a comprehensive set of federal regulations concerning genetic information seems obvious, especially in an increasingly mobile society. One can foresee that inexpensive genetic testing is on the horizon. Is it worth $200 to screen a potential employee for genetic information indicating potential health or performance issues? Is it worth $200 to acquire genetic information about a political opponent in an election and leak it to the press? Will tabloids have a field day revealing genetic information about celebrities?

It probably is an impossible task to prevent material from which genetic information can be extracted from coming into the hands of a person determined to obtain it. However, the extraction of genetic information is a task that can be performed only by persons or entities with highly specialized knowledge and equipment. In terms of protecting the privacy and appropriate use of genetic information, it makes sense to regulate those who extract the information.

Minimal concepts of regulation should include the licensing of each facility for the extraction of genetic material to assure competency and compliance with regulations and safeguards for the storage, use and dissemination of information regarding genetic material. The safeguards should include coding and restriction of identifying information and restrictions on the dissemination of information at least as stringent as currently exist for medical records.

Congress should determine whether state regulation should be pre-empted by federal regulation. In other areas, federal regulation has provided a minimum set of standards but has not pre-empted state regulation beyond the federal minimum. For example, states were free to adopt more stringent primary protections for information related to HIV than minimal protections provided by federal regulations.

On a global level, the extraction, dissemination and use of genetic information create issues for the United Nations and the world's governments. The United States

35. ARIZ. REV. STAT. § 12-2802 (2001).
36. OR. REV. STAT. § 659.715 (1996).
37. P.L. 1996, ch. 126, Genetic Privacy Act.
38. 2002 Bill Text, N.J. A.B. 1379.

will need to involve itself in an international dialogue to reach balances between the privacy interests of individuals with the interests of a variety of societies in security, health care management, or conceivably genetic engineering of multiple forms.

B. Employment

While discrimination in employment based on genetic information already is the subject of federal and state legislation and regulations, exceptions relating to the assurance of workplace health and safety or job performance requirements are exceedingly broad and trigger disputes requiring legal resolution. Employers and society clearly have an interest in assuming that airline pilots, train engineers and drivers of tractor-trailers can perform their jobs safely. Employees have substantial privacy interests in not having genetic information not legitimately related to job performance revealed to an employer or potential employer, especially if it is to reside in a personnel file for a considerable period of time.

Regulation may be useful in determining, on the basis of valid, scientific criteria, what genetic tests are reasonably related to specific job performance and providing that only genetic information related to a specific performance requirement be released to the employer. Regulation would also be useful in determining which employers can store, disseminate (if at all) or use the results of genetic tests.

C. Insurance

1. Life Insurance

Life insurance companies profit by handicapping the likelihood of a person's death. They now make discriminating decisions on whom to insure or not insure and for how much on the basis of personal and private medical information. Genetic testing will provide an additional tool for them. Should some individuals be excluded from or priced-out of the opportunity to obtain life insurance by the accident of their birth? The answer to this question is "yes" or "no" depending on one's perspective.

2. Health Insurance

There are two major issues relating to health insurance and the privacy of genetic information. One is the denial or limitation of access to health insurance based on genetic test information. The second is the potential beneficial use of broad-based genetic test information in order to direct medical research and to allocate scarce resources in the most efficient way. There is a tension between the issues.

HIPAA provides limited protection against discrimination in access to health insurance for group plans. Large numbers of persons who are not eligible for group plans have no such protection, however, and, as in the life insurance situation, societal values should determine whether genetic test results should exclude anyone from access to health insurance. The health insurance debate is beyond complex, and the introduction of genetic tests as a screening device for access to health insurance benefits or for access at an increased cost will only increase the complexity.

The accumulation of knowledge of the genetic characteristics of the population at large holds the potential for providing knowledge that could direct research having the promise to reduce or eliminate certain medical conditions or alert the medical profession to earlier intervention in the treatment of certain conditions. This knowledge may serve to reduce health care costs. But sufficient data for use in making such determinations may involve, at least in a limited sense, some surrender of genetic privacy. If government involvement in health insurance and medical research, which is already extensive, increases, then the contribution of blood for genetic testing may become the entry fee for access to health insurance.

A bank of genetic data for an extensive portion of the population might be a dream or a nightmare, depending on how it is used. If such a bank comes into existence, then stringent limitations on the use of the

data for research and the direction of research should be created in order to safeguard the privacy of the individual donors.

D. Litigation

Courts will need to address questions related to privacy rights and genetic information in a host of contexts. The Federal Judicial Center has published materials on DNA testing in the context of criminal trials,[39] but issues involving genetic testing in civil litigation will multiply.

1. Requests for Genetic Testing of Litigants

Rule 35 of the Federal Rules of Civil Procedure and similar rules in the states permit a party to seek a physical examination of an opposing litigant in appropriate cases. Requests for examinations may be accompanied by requests for certain diagnostic tests, and these might include genetic testing. In serious personal injury cases, where life care plans may project long-term care costs into the tens of millions of dollars, genetic testing may reveal information directly relevant to life expectancy issues.

In civil cases involving physical or sexual assault, genetic testing may directly relate to identity issues or to corroboration of the alleged tort.

2. Protective Orders

Where genetic testing potentially can reveal substantial private information about an individual, any request for genetic testing is likely to be met with a request for a protective order. Protective orders should address limitations on any genetic testing to relevant issues in a pending lawsuit, the confidentiality of the results of such testing, limitations on the disclosure of the results and their use in legal proceedings, and the return of records of the results after the close of litigation.

3. Limitations on Use of Lawfully Obtained Data

It is foreseeable that universities, companies involved in genetic research, governmental entities or others may, through consent for research, medical testing or other lawful means, become repositories of substantial amounts of information about the genetic background of individuals. May the holders of this information use it to target individuals for unsolicited commercial contacts concerning medical treatments or information about drugs?

The Supreme Judicial Court of Massachusetts, in a case involving a marketing campaign by a pharmacy chain to use its prescription data to target customers who had not requested the marketing material, held that a triable issue under the Massachusetts Privacy Act was presented and upheld the class certification of the plaintiffs.[40]

The use of genetic information acquired in the course of medical testing or research presents similar issues.

4. Invasion of Privacy

In situations where there has been an unlawful extraction of genetic data or unauthorized use, dissemination or publication of genetic data about an individual, there will probably be sufficient basis for an invasion of privacy lawsuit based on the principles enunciated in the Restatement (Second) of Torts.[41]

CONCLUSION

Rapid technological advances and scientific discoveries will continue to challenge the ability of governmental and judicial institutions to balance the benefit of increased knowledge with traditionally valued concepts of personal privacy and freedom.

---

39. David H. Kaye & George F. Sensabaugh Jr., *Reference Guide on DNA Evidence* in REFERENCE MANUAL ON SCIENTIFIC EVIDENCE 485 (Federal Judicial Center, 2d ed. 2000). This chapter also contains a useful glossary of terms.

40. Weld v. Glaxo Wellcome Inc., 746 N.E.2d 522 (Mass. 2001).

41. See J. Makdisi, *Genetic Privacy: New Intrusion a New Tort?* 34 CREIGHTON L. REV. 965 (2001).

The Privacy Project

Discovery Unplugged: Should Internal E-mails Be Privileged Confidential Communications?

The concept of appropriate discovery should keep pace with modern communications technology and protect intra-company e-mail

By Ralph Streza

MOST PEOPLE are more comfortable with old problems than new solutions. That notwithstanding, this article argues for the creation of a new communications privilege based on privacy and business policy: An organization's internal e-mail communications related to advancing the goals of the organization should not be discoverable in litigation, provided the organization takes the steps necessary to preserve the privacy of these communications.

DISCOVERING E-MAIL

Generally speaking, corporations, lawyers who represent corporations, lawyers who assert claims against corporations and judges who manage discovery issues related to litigation involving corporations have not questioned the propriety of allowing discovery of a company's e-mail database. It seems natural and logical for the litigation professionals to accept the discoverability of a preserved record of an individual's thoughts, or a group of individuals' exchanged thoughts, within a corporation and related to the advancement of corporate goals.

A search of the Lexis national case law database for federal and state decisions from January 1990 to the summer of 2002 uncovered no decision in which a court considered creating a privilege for internal corporate e-mail. A search of the professional journal article database covering 900 leading legal and business journals was similarly unavailing. No effort was evident in pending or abandoned federal legislation.

The evolution of computer technology in the corporate world and in society has contributed to the mindset that e-mail should be discoverable. The decisions sustaining the discoverability of e-mail, however, occurred before the practical effects of allowing that discovery were foreseen, or possibly even appreciated. The time may be ripe to rethink the propriety of invading these communications.

Responding to a discovery request for a corporation's internal e-mail sounds simple until the task begins. A corporation served with a request to produce these electronic communications will soon learn that compliance can be time consuming and very expensive. For instance, President Clinton's chief of staff, John Podesta, in October 2000 estimated that the cost of the effort to reconstruct, retrieve and analyze lost e-mail related to the Monica Lewinsky scandal would exceed $11 million. The court ordered the defendant to pay the not "undue" estimated cost in excess of $1 million to retrieve electronic data in civil litigation discovery.[1]

In addition to collecting and analyzing e-mail, the production can generate extensive

IADC member Ralph Streza is a member of Porter Wright Morris & Arthur L.L.P. in the firm's Cleveland office. He is a graduate of Miami University (B.A. 1978) and Cleveland Marshall College of Law (J.D. 1982).

1. *See* 1 *Digital Discovery & e-Evidence* at 16 (December 2000). *See also* Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass.Super.).

spin-off discovery in an effort to leave no stone unturned. An internal information technology staff can be tied up for days or even weeks, according to some treatises. If the IT staff is insufficient, the corporation must outsource the collection and analysis.[2] The e-mail may pull otherwise unknowledgeable witnesses into the litigation. They may add little, if anything, to the merits of the claims or defenses, yet they are corralled, interrogated and distracted from otherwise productive duties. Instead of uncovering truly relevant facts, e-mail productions prolong and sidetrack the search for truth, and sometimes it may even develop untruth. Some written communications found in e-mail just aren't accurate.

However, apart from these litigation-related costs, which many people argue are simply a cost of doing business, one must ask whether the true social intent, benefit and purpose of e-mail within companies, are advanced or suppressed by its use in civil litigation.

BASIS OF LEGAL PRIVILEGE

Concepts of legal privilege are grounded in private, confidential relationships. Communications made in confidence in these relationship are not protected from disclosure merely because of the confidentiality of the communication, but because of a strong public policy or a public concern that underlies the communication.[3] Privileges not to testify create narrow exceptions to the principle that the truth should be ascertained by all rational means.

Scores of articles discuss the new privacy concerns that have arisen with the advent of electronic communications. Most have centered on the privacy interests of the individual—particularly as people surf the Internet or send their encrypted message into cyberspace expecting it to land in another Internet user's mailbox. But little attention has been devoted to an organization's privacy as it relates to an intra-company e-mail network.

Legal privilege is regulated by Rule 501 of the Federal Rules of Evidence, which provides in pertinent part that the "privilege of a witness, person, government, state, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience."[4] This rule has not been amended since its adoption in 1972.

When originally submitted to Congress, Article V of the proposed Federal Rules of Evidence, of which Rule 501 is a part, listed 13 specific rules. Nine defined specific non-constitutional privileges, one expressly excluded all privileges not enumerated in Article V, and three addressed waiver issues. Ultimately, Rule 501 was adopted with the view, according to the Advisory Committee Notes, that not only were existing privileges to be applied, but that privileges would continue to develop, in light of reason and experience, and that "the recognition of a privilege based on a confidential relationship and other privileges should be determined on a case-by-case basis."

It seems settled that an organization has a reasonable expectation of privacy in its closed e-mail system implemented to exclude third parties to allow its employees to communicate.[5] It also is undisputed that

---

2. *Digital Discovery & e-Evidence*, *supra* note 1, at 4.

3. 81 AM. JUR. 2D *Witnesses* § 286 (1992) states: "It must appear that the element of confidentiality is essential to the full and satisfactory maintenance of the relation between the parties, the relation must be one which in the opinion of the community ought to be sedulously fostered, and the injury that would inure to the relation by the disclosure of the communication must be greater than the benefit thereby gained for the correct disposal of litigation."

4. Many states have adopted the "reason and experience" guideline of Rule 501. Twenty-six states have adopted this rationale, a rule patterned after Article V or similar provisions. 23 CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., FEDERAL PRACTICE AND PROCEDURE: EVIDENCE § 5421 (2d ed. 1982 & Supp. 2002).

5. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 236 (1986), *aff'g* 749 F.2d 307 (6th Cir. 1984) (well settled that business that undertakes extensive effort to protect interior of its business from un-

the closed e-mail network belongs to the corporation and not to the employees who use it.[6] At least one court has determined that the expectation of privacy related to e-mail is linked to the type of e-mail involved and the intended recipient. By negative inference from that decision, the users of a closed network have a much greater privacy right in a closed network.[7]

APPLICATION TO E-MAIL

Accepting the premise that communications given in the closed network are confidential and private, one must remember the goals of e-mail. E-mail is a shorthand way of expressing a thought with the added benefit that the other side of the communication does not need to be present for the thought to be sent or received. E-mail often is a fleeting thought, unintentionally memorialized. While there sometimes is ample time to alter the thought, there is seldom corrective follow-up or retraction.[8]

In a very real sense, an e-mail is, at most, half of a conversation, and its reliability for the truth of its content is suspect for many reasons. For example, in a conversation, there is give and take, feedback in the form of questions, and pauses and voice inflections that provide personal cues to the interpretation of the message. Ideas are often modified or discarded during the conversation. By contrast, in an exchange of e-mail thoughts, when an idea is changed, there is not always a written acknowledgment of that change.

E-mail users often communicate in an informal and casual manner, not taking the care usually invested when writing a formal business document. Users often believe that once a message is communicated and deleted, it disappears forever, much like a telephone call when the communication has ended. As a result, a discovering party may find a variety of candid statements made about company strategies and secrets that would never have been presented on paper.[9]

Even if deleted, e-mail still can be recovered, and if deleted e-mail is requested and produced, consideration must be given to the reason for the deletion. It is quite possible that the person deleting the e-mail changed his or her mind about the content of the e-mail. Yet, an after-the-fact explanation may not be convincing.

Despite its compromised reliability in litigation, intra-company e-mail networks are useful to a corporation. One court has recognized that companies not only incur enormous expense in implementing the technology to stay competitive, they then face substantial expense to produce the data based on a concept of "litigation fairness."[10] E-mail has become as basic to most companies as the telephone, and in most setting has overtaken the telephone as the preferred method to communicate.

Although e-mail discovery has been allowed in civil cases, it is ironic that the same invasion into the content of private conversations—with or without a telephone—generally has not been allowed,

---

wanted intrusions from public or competitors "has a reasonable, legitimate and objective expectation of privacy within the interior of its covered buildings, and it is equally clear that expectation is one society is prepared to observe").

6. *See* Smith v. Pillsbury Co., 914 F.Supp. 97 (E.D. Pa. 1996) (company-owned e-mail system belongs to company, not to employees using system, thereby distinguishing situations that involve employees who claim invasion of their privacy when company disciplines or discharges employee for abusing or misusing company e-mail system).

7. *See* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996). In this case, the court analyzed the scope of privacy related to e-mail transmitted via an Internet online service provider (AOL) in a criminal case of distributing child pornography by the defendant under an anonymous screen name.

8. *See* Connie W. Crook & Rosemary Booth, *Building Rapport in Electronic Mail Using Accommodation Theory*, SOC'Y FOR ADVANCEMENT OF MANAGEMENT J., Winter 1997, at 4: "In electronic communication, the rapidity of response, the jargon and symbols used, and the informality of the message give additional meaning to the communication. Thus, to communicate effectively the author must accommodate the message to the reader by adjusting it to reflect the reader's communication style."

9. Armen Artinyan, *Legal Impediments to Discovery and Destruction of E-mail*, 2 J. LEGAL ADVOC. & PRAC. 95, 96 (2000).

10. In re Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526 (N.D. Ill.).

and evidence based on that invasion generally is not admissible.[11] It is unlawful for anyone to intercept the conversation of third parties with wiretaps or listening devices, unbeknownst to those talking. Such conduct otherwise might give rise to a private cause of action for damages as an invasion of privacy, and in some jurisdictions it is a criminal offense. The "fruit" of a subpoena or request for production of e-mail is fundamentally the same as the fruit of a wiretap or the illegal capture of conversation.

Courts have declined to admit illegally obtained evidence by way of wiretap in civil litigation.[12] Even where the wiretap was authorized by law in the context of a criminal investigation, courts have refrained from allowing civil litigants from discovering the recorded conversation.[13] No case could be found in which a court issued a wiretap order to help civil litigants discover their claims or prepare their defenses.

NEVERTHLESS, PRODUCTION ORDERED

Despite these issues, corporations have been required and presumably will continue to be required to produce e-mail. The presumption that e-mail should be discoverable and admissible has developed a business mindset that discovery is a factor in a company's decision to employ an internal e-mail communication system: "Technology should be easily adaptable once litigation has begun and discovery orders have been issued. Wise technology decisions may make compliance with discovery smooth and affordable; poor strategic planning can make it onerous and expensive."[14]

The production of deleted computerized information is also part of the expense.[15] This has generated extensive efforts to ensure that corporations responsibly manage internal e-mail and other computerized data so that when a discovery request arrives, the company will not have to sift through millions of pages of disorganized data to determine the content of the data. Spoliation of evidence has generated million dollar fines when a company failed to preserve electronic data that harmed a claimant's ability to establish its claims.[16]

CONCLUSION

This article is intended to catalyze continued discussions on the benefits and burdens of intra-company e-mail productions. Underlying this rethinking is the question whether our concept of appropriate discovery has kept pace with this communication technology. The search for truth in the civil discovery process existed for many years before the advent of e-mail. The costs and burdens on companies, as well as the arguable defeated purpose of e-mail generally, might outweigh the benefits to have been gained by discovery into intra-company e-mail. If that is the case, then this may require a fundamental rethinking of whether intra-company e-mail should not be included in the litigation process.

---

11. *See* Katz v. United States, 389 U.S. 347, 353 (1967), *rev'g* 369 F.2d 130 (9th Cir. 1966) (use of eavesdropping devices without warrant violates Fourth Amendment when speaker has reasonable expectation of privacy).

12. *See, e.g.*, Filosa v. Filosa, 1991 WL 180392 (E.D. N.Y.). The court relied on the prohibition in 18 U.S.C. § 2515 on the use of illegally obtained wiretap evidence or evidence derived therefrom in "any trial, hearing, or other proceeding in or before any court." *See also* United States v. Wuliger, 981 F.2d 1497 (6th Cir. 1992) (declining to recognize impeachment exception to 18 U.S.C. § 2515 to allow use of illegally obtained wiretap in civil proceedings between private parties).

13. *See* In re Motion to Unseal Electronic Surveillance Evidence, 990 F.2d 1015, (8th Cir. 1993) (18 U.S.C. § 2517 does not authorize pretrial disclosure of wiretap evidence to private civil litigants). S*ee also* Nat'l Broadcasting Co. v. U.S. Dep't of Justice, 735 F.2d 51 (2d Cir. 1984) (finding lack of authority to compel government to release recorded tapes to private litigant pursuing civil matter).

14. William DeCoste, *Sender Beware: The Discoverability and Admissibility of E-mail*, 2 VAND. J. ENT. L. & PRAC. 79, 84 (2000).

15. *See* Gregory I. Rasin & Joseph P. Moan, *Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace*, 66 MO. L. REV. 793, 799 (2001).

16. *See* In re Prudential Ins. Co. Sales Practices Litig., 169 F.R.D. 598, 617 (D. N.J. 1997).

The Privacy Project

The Self-critical Analysis Privilege in the Product Liability Context

If analyzed as a subsequent remedial measure, self-evaluation wouldn't impede discovery, but the information would be protected

By George S. Hodges, Karen A. Jockimo and Paul E. Svensson

IT IS self-evident that any business should emphasize self-critical analysis of its significant operations and products in order to deliver safe and effective products to its consumers. The opportunity to gain increased market share, maintain lower insurance premiums and avoid both the high costs of litigation and potential adverse judgments co-exist as tangible benefits.

Trouble arises when a company undertakes self-examination, evaluates or makes a product modification, and litigation still arises from a prior event. The principal issue becomes whether the party bringing suit should have access to any of the information discovered through the self-examination. Or is that information privileged? To date, only a few courts and commentators have considered the application of the self-critical analysis privilege in the product liability context.

HISTORICAL PERSPECTIVES

A. Judicial Review

Self-critical analysis has developed in the United States over the years as a federal common law privilege based on the application of Federal Rule of Evidence 501, which states:

> Except as otherwise required by the Constitution of the United States or provided by act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, state, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings with respect to an element of a claim or defense as to which state law supplies the rule of decision, the privilege of a witness, person, government, state, or political subdivision thereof shall be determined in accordance with state law.

The privilege is premised on the public policy that frank and potentially damaging self-criticism should be protected from discovery in order to encourage this socially beneficial activity.[1] This is particularly true where businesses seek to review and improve on the safety of its products. The underlying theory is that if discovery is al-

IADC member George S. Hodges is managing partner of Boeggeman, George, Hodges & Corde, P.C., of White Plains, New York, and a member of the IADC Executive Committee. He is a graduate of Fordham University (B.A. 1970; J.D. 1973).

Karen A. Jockimo is a partner in the same firm. She was educated at Connecticut College (B.A. 1989) and Pace University School of Law (J.D. 1993).

Paul E. Svensson received his J.D. from Pace University School of Law in 2002. He also was educated at the University of Pittsburgh (M.P.H. 1979 and Holy Cross College (B.A. 1976).

1. Sheppard v. Consol. Edison Co., 893 F.Supp. 6, 7 (E.D. N.Y. 1995) ("disclosure of documents reflecting candid self-examination will deter or suppress socially useful investigations and evaluations or compliance with the law").

lowed, there may be a "direct chilling effect on the institutional or individual self-analyst; and that this effect operates to discourage the analyst from investigating thoroughly and frankly or even from investigating at all."[2] This concern becomes even more meaningful where corrective measures can only be cultivated from self-examination of the type the privilege is expected to protect.

Unfortunately, the playing field facing U.S. businesses over the past decade largely has been an uneven landscape. Neither the Constitution, the Congress, nor the U.S. Supreme Court has expressly created a self-critical analysis privilege. The Court's decisions in *University of Pennsylvania v. Equal Employment Opportunity Commission*[3] and *Trammel v. United States*[4] indicate that the application of a self-critical analysis privilege should be decided on a case-by-case basis.

In judicial review, the privilege often falls under severe scrutiny, resulting in its uncertain application, thus thwarting the candor with which such evaluations are intended to be performed and deterring corporations from proceeding with self-critical studies.

Judicial reluctance to extend the self-critical analysis privilege and the resultant unpredictability of the privilege's application to internal analytical reviews have prompted commentators to advocate proposals for codifying a broad self-critical analysis privilege.[5] However, as is the case with Congress, at the present time there is no state legislation addressing a self-critical privilege in regard to product safety review activities and nothing meaningful under discussion.

B. Development of Privilege

The self-critical analysis privilege was first recognized in 1970 in the context of a medical malpractice action. In *Bredice v. Doctor's Hospital*, an administratrix, on behalf of the decedent, sued the hospital for malpractice. The plaintiff moved for the production and inspection of minutes and reports of any board or committee of the hospital or its staff concerning the death of the decedent and of reports, statements or memoranda, including reports to the malpractice insurance carrier pertaining to the deceased or his treatment, no matter when, to whom or by whom made. In essence, the plaintiff was attempting to obtain the minutes of a hospital peer review meeting at which the decedent's care was evaluated.

The U.S. District Court for the District of Columbia denied access to the minutes, relying on the public policy rationale underlying the self-critical or self-evaluative privilege. The court noted:

> Confidentiality is essential to effective functioning of the staff meetings; and these meetings are essential to the continued improvement of the care and treatment of patients. Candid and conscious evaluation of clinical practices is a sine qua non of adequate hospital care. To subject these discussions and deliberations to the discovery process, without a showing of exceptional necessity, would result in terminating such

---

2. *See* Note, *The Privilege of Self-critical Analysis*, 96 HARV. L. REV. 1083, 1091-92 (1983) (explaining that direct chilling effect not only includes fear of lawsuits, but also that analyst may "temper his criticism out of a fear that reprisals will result" if result is liability).

3. 493 U.S. 182 (1990), *aff'g* 850 F.2d 969 (3d Cir. 1988) (refusing to recognize peer review privilege relative to employment documents). The Supreme Court, however, has recognized privileges similar to the privilege of self-critical analysis on at least three occasions: United States v. Nixon, 418 U.S. 683 (1974), *aff'g* 377 F.2d 1326 (D. D.C. 1974) (qualified privilege for Presidential communications); Nat'l Labor Relations Bd. v. Sears, Roebuck & Co., 421 U.S. 132 (1975) (construing exception to Freedom of Information Act in which Congress incorporated well-established privilege for deliberative intra-agency documents); Douglas Oil Co. v. Petrol Stops Northwest, 441 U.S. 211 (1979), *rev'g* 571 F.2d 1127 (9th Cir. 1978) (recognizing privileged nature of grand jury proceedings).

4. 445 U.S. 40, 47 (1980), *aff'g* 583 F.2d 1166 (10th Cir. 1978).

5. *See, e.g.*, Paul B. Taylor (Note), *Encouraging Product Safety Testing by Applying the Privilege of Self-Critical Analysis when Punitive Damages Are Sought*, 16 HARV. J.L. & PUB. POL'Y 769, 796-97 (1993); David P. Leonard, *Codifying a Privilege for Self-critical Analysis*, 25 HARV. J. ON LEGIS. 113, 117 (1988).

> deliberations. Constructive, professional criticism cannot occur in an atmosphere of tension that one doctor's suggestion will be used as a denunciation of a colleague's conduct in a malpractice suit."[6]

The court also noted that the purpose of the hospital's staff meetings was to improve, through self-analysis, the efficiency of medical procedures, techniques and patient care. Without an ability to conduct a retrospective review, the value of these types of meetings would be undermined if they and the names of those participating were to be opened to discovery.

The *Bredice* rationale for refusing to disclose the minutes and reports of hospital staff meetings was adopted by the U.S. District Court for the Northern District of Georgia in *Banks v. Lockheed-Georgia Co.*[7] The *Banks* court held that disclosure of information concerning a company's candid self-analysis, which evaluated its employment practices and affirmative action compliance programs, would have a discouraging effect on equal employment opportunities.

The *Banks* court concluded that "it would be contrary to [public] policy to discourage frank self-criticism and evaluation in the development of affirmative action programs of this kind." The court also relied on the reasoning of *Bredice* and noted that to allow "access to the written opinions and conclusions of the members of Lockheed's own research team would discourage companies such as Lockheed from making investigations which are calculated to have a positive effect on equalizing employment opportunities."

Since the self-critical analysis privilege was first recognized judicially in *Bredice* and *Banks*, it has been extended to numerous areas including accounting records;[8] securities losses;[9] academic peer reviews;[10] railroad accident investigations;[11] product safety assessments;[12] and products liability.[13]

The rationale behind applying the self-critical analysis privilege in these situations has essentially been the same: "It allows individuals or businesses to candidly assess compliance with regulatory and legal requirements without creating evidence that may be used against them by their opponents in future litigation."[14]

A QUALIFIED PRIVILEGE

In determining whether a self-critical analysis privilege will apply, courts have followed no single rule, test, analysis or evaluation. In fact, it is clear that the self-critical analysis privilege is a qualified one whose application cannot be guaranteed under any circumstances. The three criteria historically considered by courts include:

- Whether the information resulted from critical self-analysis taken by the parties seeking protection;
- Whether the public has a strong interest in preserving the free flow of the type of information sought; and
- Whether the information is of a type whose flow would be curtailed if discovery were not allowed.

The burden of establishing that these criteria have been meet is on the party seeking to assert the self-critical analysis privilege. Meanwhile, courts also have created numerous limitations and restrictions on the self-critical analysis privilege.

First, a document generally will not be accorded this privilege unless it was prepared with the expectation that it would be kept confidential and, equally as important, has been kept confidential. This limitation was first enunciated in *Dowling v. American Hawaii Cruises*.[15] In *Dowling*, the

---

6. 50 F.R.D. 249, 250 (D. D.C. 1970), *aff'd*, 479 F.2d 920 (D.C. Cir. 1973).
7. 53 F.R.D. 283 (N.D. Ga. 1971).
8. New York Stock Exch. v. Sloan, 489 F.2d 1 (2d Cir. 1973).
9. Crazy Eddie Sec. Litig., 792 F.Supp. 197 (E.D. N.Y. 1992).
10. Keyes v. Lenori Rhyne College, 552 F.2d 579 (4th Cir.), *cert. denied*, 443 U.S. 904 (1977)
11. Granger v. Nat'l R.R. Corp., 116 F.R.D. 507 (E.D. Pa. 1987).
12. Lloyd v. Cessna Aircraft Co., 74 F.R.D. 518 (E.D. Tenn. 1977)
13. Bradley v. Melroe Co., 141 F.R.D. 1 (D. D.C. 1991)
14. Reichhold Chemicals Inc. v. Textron Inc., 157 F.R.D. 522, 524 (N.D. Fla. 1994).
15. 971 F.2d 423 (9th Cir. 1992).

Ninth Circuit was asked to determine whether the plaintiffs could discover the minutes of meetings of a ship safety committee held prior to a crewman's injury. The ship had asserted that the documents were protected by the self-critical analysis privilege. In addition to applying the three criteria above, the court also considered whether the documents were prepared with the expectation that they be kept confidential.

The *Dowling* court ultimately concluded that the documents should not be given the benefit of the self-critical analysis privilege, holding that routine safety inspections would not be curtailed merely because they might be subject to future disclosure. Moreover, the court did not believe that routine safety inspections were normally performed with the expectation that they would be kept confidential.[16]

Thus, the *Dowling* court applied a fourth prong to the historical self-critical analysis privilege test by requiring that any self-evaluative documents be created with the intent that they be confidential and be kept confidential. As a consequence, it is often recommended that an evaluator conspicuously mark self-critical documents as confidential and that the internal and external distribution of the documents be limited in order effectively to limit their disclosure.[17] Since *Dowling*, some federal courts have applied this test, while others have not.

The privilege also has been limited to the extent that it has been held to apply only to subjective impressions and opinions exercised in evaluating the product and not to statistical or objective facts regarding use of the product.[18] Additionally, the privilege has been found inapplicable in a circumstance where the document has been subpoenaed by a government agency as part of an administrative review.[19]

Finally, it has been held that the self-critical analysis privilege is a qualified one that can be overcome by a showing to the court of "extraordinary circumstances or special need."[20] Thus, as in the application of the attorney work product privilege, a litigant seeking disclosure of a document from a possessor asserting the self-critical analysis privilege may overcome the privilege by showing extraordinary circumstances and special need. It has been argued that to allow a party to overcome the privilege by showing exceptional needs risks the evisceration of the privilege itself. Proponents of a legislatively mandated self-critical analysis privilege contend that allowing such limitations to the privilege leaves businesses that conduct self-critical analysis "uncertain of their protection."[21]

PRODUCT LIABILITY DECISIONS

Claims of self-critical privilege have been reviewed consistently under Rule 501 of the Federal Rules of Evidence, but the tests applied by the various federal courts have varied in part because of the application of state common law when jurisdiction is based on diversity of citizenship.[22] In the state courts, the application of a self-critical analysis privilege has been considered under state evidence law based on Rule 501, as well as the test recognized by the applicable state common law. In doing so, some state courts have recognized this privilege,[23] while others have not.[24]

---

16. *See also* Reichhhold, 157 F.R.D. 522.

17. *See* Note, *Legal Development: The Privilege of Self-critical Analysis: A Survey of the Law*, 60 ALB. L. REV. 171 (1996).

18. Webb v. Westinghouse Elec. Corp., 81 F.R.D. 431, 433-35 (D. Pa. 1978); Reed Lockheed Aeronautics, 199 F.R.D. 379 (N.D. Ga. 2001).

19. Fed. Trade Comm'n v. TRW Inc., 628 F.2d 207, 210 (D.C. Cir. 1980).

20. *See, e.g.*, Mao-Shiung Wei v. Bodner, 127 F.R.D. 91 (D. N.J. 1989). *See also* Bredice, 50 F.R.D. 249.

21. *See* Note, *Privilege of Self-critical Analysis*, *supra* note 2.

22. *See, e.g.*, Lawson v. Fisher-Price, 191 F.R.D. 381 (D. Vt. 1999).

23. Kansas Gas & Elec. v. Eye, 789 P.2d 1161 (Kan. 1990) (discussing Berst v. Chapman, 653 P.2d 107 (Kan. 1982), in which the Kansas Supreme Court recognized the self-critical analysis privilege); Anderson v. Hahnemann Med. Coll., 1985 WL 47218 (Pa.Commw.Ct.).

24. Payton v. New Jersey Turnpike Auth., 691 A.2d 321 (N.J. 1997) (self-critical analysis does not exist in common law but court may consider it in balancing need for discovery against prejudice to party resisting it); Univ. of Ky. v. Courier-Journal & Louisville Times Co., 830 S.W.2d 373 (Ky. 1992);

A. State Courts

Of the state cases, only *Limite v. Emerson Electric Co.—White Rodgers Division* involved litigation related to the disclosure of product safety information.[25] The New York Appellate Division affirmed an order compelling discovery of all documents created during an investigation by the federal Consumer Product Safety Commission. The court held that a section of the Consumer Product Safety Act mandating nondisclosure of CPSC investigations was inapplicable to judicial proceedings based on its plain language.

The *Limite* court also modified the order of the trial court to protect all information in the documents disclosed by Emerson Electric to the plaintiff from public disclosure, but the plaintiff was provided with Emerson Electric's self-critical analysis to use in developing its case and subsequently at trial. The court opined that any danger to the defendant's reputation as a manufacturer from plaintiffs' access to incomplete or inaccurate information should be obviated by an appropriate protective order, thus complying with the legislative intent of the statute.[26]

There have been other New York decisions recognizing privileges similar to a self-critical analysis privilege, but none of these dealt with product safety issues.[27]

B. Federal Courts

Federal courts historically have been concerned with a vexing dilemma between the interest in disclosure that is expected to "contribute to full and fair determination of all facts relevant to the plaintiff's claims," and the importance of maintaining "confidentiality both to assure fairness to persons who have been required by law to engage in self-evaluation . . . and to make the self-evaluation process more effective by creating an effective incentive structure for candid and unconstrained self-regulation."[28] The federal cases reviewed below addressed the self-critical analysis privilege involving both the protection of pre-accident and post-accident reviews, as required by the Consumer Product Safety Act,[29] and with the protection of documents produced in the course of self-evaluation.

In contrast to the New York decisions, the federal courts in *Shipes v. BIC Corp.*,[30] *Roberts v. Carrier Corp.*[31] and *Ashley v. Uniden Corp.*[32] endorsed the self-critical analysis privilege and applied it to confidential self-evaluation documents created by a manufacturer for submission to the CPSC. A state court case, *Scroggins v. Uniden Corp.*,[33] decided shortly after *Rob-*

Scroggins v. Uniden Corp. of Am., 506 N.E.2d 83 (Ind.App. 1987) (Indiana courts recognize only statutory privileges); Southern Bell Tel. & Tel. Co. v. Beard, 597 So.2d 873 (Fla.App. 1992) (all privileges in Florida are statutory, thus no common law privilege for self-critical analysis exists); Combined Communications Corp. v. Pub. Serv. Co. of Colorado, 865 P.2d 893 (Colo.App. 1993) (self-critical analysis privilege does not exist in Colorado, although court applied self-critical analysis to case and held that it did not apply); Cloud v. Superior Court (Litton Indus. Inc.), 58 Cal.Rptr.2d 365 (Cal.App. 1996), (self-critical analysis privilege not in state evidence code, thus does not exist in California); Grimes v. DSC Comm. Corp., 724 A.2d 561 (Del.Ch. 1998); Harris-Lewis v. Mudge, 1999 WL 98589 (Mass.Super. 1999); Office of Consumer Council v. Dep't of Pub. Util. Control, 665 A.2d 921 (Conn.Super. 1994); Lamite v. Emerson Elec. Co.—White Rodgers Div., 535 N.Y.S.2d 650 (App.Div. 3d Dep't 1988), *leave to appeal dismissed*, 74 N.Y.2d 650 (1989) (permitting disclosure for purposes of litigation but barring any public dissemination of information).

25. 535 N.Y.S.2d 650, *supra* note 24.

26. *See also* Consumer Prod. Safety Comm'n v. GTE Sylvania Inc., 447 U.S. 102, 111-13 (1980), *aff'g* 598 F.2d 790 (3d Cir. 1979).

27. Martin v. Gross, 605 N.Y.S.2d 742 (App. Div. 1st Dep't 1993) (applying public interest privilege to child protective services records); One Beekman Place Inc. v. City of New York, 564 N.Y.S.2d 169 (App.Div. 1st Dep't 1991) (applying privilege of communication between public officers regarding zoning determination).

28. O'Connor v. Chrysler Corp., 86 F.R.D. 211, 218 (D. Mass. 1980).

29. 15 U.S.C. §§ 2051-83. For another example of regulation with ramifications in the products liability area, *see* Patricia L. Andel, *Inapplicability of the Self-critical Analysis Privilege to the Drug and Medical Device Industry*, 34 SAN DIEGO L. REV. 93 (1997) (advocating inapplicability of privilege to drug and medical device industry, which is subject to federal Food, Drug, and Cosmetic Act and Freedom of Information Act).

30. 154 F.R.D. 301 (M.D. Ga. 1994).

31. 107 F.R.D. 678 (N.D. Ind. 1985).

32. 1986 U.S.Dist. Lexis 22409 (W.D. Tex.).

33. 506 N.E.2d 83 (Ind.App. 1987).

erts and *Ashley*, declined to recognize a non-statutory privilege, and *Lawson v. Fisher-Price Inc.*,[34] another federal court case, also did not recognize the privilege.

1. Shipes

In *Shipes*, jurisdiction was based on diversity, and the U.S. District Court for the Middle District of Georgia applied the test favored in that state. The court noted that Georgia's self-critical privilege statute is applicable only to "medical peer review" activities.[35] However, it reviewed the analysis of the federal common law privilege that had been conducted in *Banks* by the federal court for the Northern District of Georgia. The *Shipes* court concluded that the reasoning behind the federal common law privilege for self-critical analysis mirrors that supporting the Georgia statutory medical peer review privilege and that the public interest is furthered when organizations or corporations critically analyze their safety records.

Under the test applied in Georgia, which was derived from the Ninth Circuit decision in *Dowling*, the party asserting the privilege must meet four criteria:

> "First, the information must result from a critical self-analysis undertaken by the party seeking protection; second, the public must have a strong interest in preserving the free flow of information sought; [third], the information must be of the type whose [creation] would be curtailed if discovery were allowed" . . . Additionally, the document must have been created with the expectation that it would be kept confidential and must have remained so.[36]

The *Shipes* court also recognized that federal courts have applied two different tests when evaluating a party's claim of a self-critical privilege. It reviewed the test used by the district court in Indiana in *Roberts*, which held that for the materials to be privileged: (1) they must have been prepared for mandatory government reports; (2) the privilege only extends to subjective, evaluative materials; (3) the privilege does not extend to objective data in the same reports; and (4) discovery should be denied only where the policy favoring exclusion has clearly outweighed plaintiff's need.[37] The *Shipes* court concluded that regardless of which test was applied in the case before it, the same conclusion is reached.

The *Shipes* court reasoned that since the documents were equivalent to "medical peer review" under Georgia law because they were submitted to the CPSC pursuant to the Consumer Product Safety Act, they were entitled to the self-critical analysis privilege. However, the court held that the documents must have been specifically created for submission to the review agency in order to be privileged and that information, documents or records otherwise available from original sources are not immune from discovery merely because they were sent to the reviewing agency. The court added that the material would not be privileged unless it was subjective and evaluative; thus, factual material would be discoverable.

The determination that factual material is not protected by the self-critical analysis privilege is consistent with federal court decisions. It also is well settled that the privilege, when recognized, must be balanced against the party's need for full and fair discovery to determine the issues in the litigation.[38] In a majority of cases, the fed-

---

34. 191 F.R.D. 381 (D. Vt. 1999).

35. GA. CODE ANN. § 31-7-143; Hollowell v. Jove, 270 S.E.2d 430 (Ga. 1981) (materials generated in course of medical review committee proceedings concerning physician's competence protected from discovery in civil lawsuits).

36. 154 F.R.D. at 307, *quoting* Dowling, 971 F.2d at 426. *Compare* Roberts, 107 F.R.D. at 684 (setting forth different four-part test for self-critical analysis).

37. 107 F.R.D. at 684. *See also* Resnick v. Am. Dental Ass'n, 95 F.R.D. 372, 374 (N.D. Ill. 1982).

38. Fischer v. Borden, 1994 U.S.Dist. Lexis 21275 (D. N.J.) (buyer's internal inspection reports were not protected because information they contained was factual, reviews were not made with eye to being kept confidential, and buyer would not stop making them as result of disclosure); Bradley, 141 F.R.D. 1 (mental impressions, opinions, evaluations, recommendations and theories of investigatory files privileged but factual material discoverable); Lloyd, 74 F.R.D. 518 (disallowing discovery of minutes and memoranda of meetings concerning self-evaluation of possible negligent manufacture of products).

eral courts have recognized a privilege of self-critical analysis precluding the discovery of impressions, opinions and evaluations, but allowing discovery of factual data.

Although there is some danger that the factual information will be used to develop litigation, critical evaluation is protected because the ultimate benefits far outweigh any benefits of disclosure, and thus the evaluation itself is limited from public exposure, because it is not realistic to expect candid expressions of opinion or suggested changes in policies, procedures or processes when people know that such statements or suggestions may very well be used against colleagues and employees in subsequent litigation.[39]

2. Roberts

In *Roberts*, the federal district court for the Northern District of Indiana acknowledged the applicability of a self-critical analysis privilege to a post-accident report review required by federal law, but it refused to apply it to the voluntary disclosure by the manufacturer to the Consumer Product Safety Commission. The *Roberts* court applied a slightly different test from that used by the *Shipes* court, focusing on the condition that the material sought to be privileged must be prepared for mandatory reports to the government. The distinction from the *Dowling* and *Shipes* tests is clear. Instead of covering any material produced in critical self-analysis, *Roberts* required that the material be mandated by operation of law. Thus, any self-critical analysis conducted by the business entity to improve its product, but not mandated by law, would be unprotected.

As a consequence, the test applied in *Roberts* does not allow a business to engage confidentially in the type of pre-accident review activity found by the *Dowling* and *Shipes* courts to be protected by the privilege. Instead, the court interpreted the public policy behind the self-critical analysis privilege "'to assure fairness to persons required by law to engage in self-evaluation . . . and to make the self-evaluation process more effective by creating an effective incentive structure for candid and unconstrained self-evaluation.'"[40] Applying this standard to the facts of its case, the court concluded that any document not specifically prepared for and turned over to the Consumer Product Safety Commission enjoyed no privilege.

Although the information was turned over voluntarily to the commission, the *Roberts* court held that since it was originally prepared "in the regular course of business," it was not entitled to protection because it was not prepared specifically as a government-required report. The court borrowed this holding from an employment discrimination case, as this was the first federal court to consider the application of the self-critical analysis privilege in a product safety context. The court refused to accept the defendant's argument that public policy favored protecting self-critical analysis as an incentive for businesses to conduct such an analysis without fear of subsequent reprisal. It interpreted the plain language of the Consumer Product Safety Act as requiring businesses to report any defective condition discovered. Thus, the court reasoned that any damaging information would be protected under this express test.

However, the risk that information can be gathered before evidence of a defective condition is known, and that this information may be used to develop litigation, creates a strong disincentive, contrary to public policy, to study a product critically before an accident occurs. The interpretation by *Roberts* of the plain language of the statute must be clearly distinguished when counsel seeks to protect post-accident information.

3. Ashley

In *Ashley*, the U.S. District Court for the Western District of Texas addressed a

---

39. *See* Bradley, 141 F.R.D. at 3, citing William B. Johnson, Annotation, *Discoverability of Traffic Accident Reports and Derivative Information*, 84 A.L.R.4th 15, 24 (1991).

40. 107 F.R.D. 684, *quoting* O'Connor, 86 F.R.D. at 218.

plaintiffs' motion to compel the defendant to state what efforts it made to comply with Section 15 of the Consumer Product Safety Act. The defendant refused to answer the interrogatory on the ground of the common law privilege against the disclosure of critical self-analysis.

Ashley follows the test of *Roberts*. The court acknowledged that the privilege arises with respect to materials containing subjective, evaluative information that have been prepared as part of a mandatory report to a governmental agency when the factors favoring exclusion clearly outweigh a plaintiff's need for the information. The court also recognized that the regulations issued under the act encourage manufacturers to engage in critical self-analysis and to err on the side of reporting. The court reasoned that 15 U.S.C. § 2064(b) and the regulations promulgated thereunder encourage a manufacturer to issue a report even where the manufacturer might doubt the existence of a defect.[41]

More important, the *Ashley* court recognized that the need to encourage full and frank disclosure of information to the government regarding defective products is of crucial importance to the consuming public. The court opined that the success of the reporting scheme would be severely undercut if manufacturers feared that their frank disclosures might be used against them in lawsuits.

Ashley concluded that reporting itself comes within the privilege of critical self-analysis. The court reasoned that the same policy considerations that dictate non-disclosure of critical self-analysis also dictate non-disclosure of the very fact of reporting. The court stated that the mere fact that a manufacturer has reported that its product might have a defect can be just as damaging before a jury as the very details of the defect.

4. Scroggins

In *Scroggins*, decided shortly after *Roberts* and *Ashley*, the Indiana Court of Appeals held that in Indiana all privileges are statutory in nature and that there was no privilege against production of self-critical analysis. It is the role of either Congress or the state legislature to create such a privilege, the court declared, not its prerogative. The court opined that "a responsible manufacturer who discovered a dangerous article and filed a self-critical analysis reflecting the danger, would cease distribution of it, or at least be ordered to cease and desist" by the Consumer Product Safety Commission. The court failed to conduct any search of the literature or conduct any discovery to support its assumption that a self-critical analysis necessarily required a product recall, even though the case involved the same defendant as in *Ashley*.

5. Lawson

In *Lawson*, the most recent product safety case to be considered by the federal courts, the Vermont federal district court held that information submitted to the Consumer Product Safety Commission prior to the subject accident was not protected by the self-critical analysis privilege. Jurisdiction was based on diversity and the court was bound to apply Vermont law. The test used in Vermont differs from that under both *Roberts* and *Shipes*, and the court engaged in no discussion as to the findings in these cases, the implications of these findings on the case before it, or the divergence in the tests as applied by the different courts.

The *Lawson* court concluded that, under Vermont law, the following four-part test for recognition of a discovery privilege

41. 15 U.S.C. § 2064(b) provides: "Every manufacturer of a consumer product distributed in commerce, and every distributor and retailer of such product, who obtains information which reasonably supports the conclusion that such product—(1) fails to comply with an applicable consumer product safety rule; or (2) contains a defect which could create a substantial product hazard described in subsection (a)(2) of this section, shall immediately inform the commission of such failure to comply or of such defect, unless such manufacturer, distributor, or retailer has actual knowledge that the commission has been adequately informed of such defect or failure to comply."

must be applied: (1) The communications must originate in a confidence that they will not be disclosed. (2) This element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties. (3) The relation must be one that in the opinion of the community ought to be sedulously fostered. (4) The injury that would inure to the party by the disclosure of the communications must be greater than the benefit gained for the correct disposal of litigation. The party seeking creation of the privilege has the burden of satisfying the four conditions and must meet all four before the privilege will be recognized.

At first, the Vermont court's test seems to be a broader application of the test applied in *Roberts* and *Ashley*. Instead of limiting protection to government mandated reports, on its face this test would allow materials prepared in confidence and for the purposes of monitoring product safety to be privileged, particularly if the materials were subsequently disclosed to the Consumer Product Safety Commission. Moreover, these materials need not be limited to evaluations, but they theoretically could include factual data as well. Both the *Lawson* and *Roberts-Ashley* tests allow for a balancing of public policy interests in fair litigation practice and on-going product safety evaluation by the court.

The test as applied in *Lawson* reflects few of those characteristics, thus making the absence of reference to *Roberts*, *Shipes* and *Ashley* all the more puzzling. The court held that the information submitted to the CPSC failed to meet the test, reasoning that although the communication did originate in a confidential situation, since the commission rules restricting disclosure assured the investigated party that produced materials will not be lightly disclosed, such confidentiality "does not appear to be essential to the full and satisfactory maintenance of the relation between the parties as required by the second prong" of the test.

However, the court viewed this prong only from the perspective of the commission, indicating that the commission's relationship and dependence on the accurate reporting of information will not be undercut by subsequent disclosure of that material in litigation. "The reporting of certain information about potential product defects to the [commission] is mandated by law; thus, a company's refusal to compile and disclose materials to [the commission] out of fear of subsequent public disclosure would simply be illegal," the court stated.[42]

The court also held that the information under review failed the last two prongs of the test because, while it appeared important to foster the relationship between corporations and the commission, the mandatory nature of reporting mitigated the need to develop a strong relationship between the two parties. In doing so, the court totally neglected to recognize that the provision of self-critical information, not subject to disclosure, was integral to the relationship between the parties as created by operation of law.

WHERE ARE WE GOING?

A. Case Law

One may wonder what rhyme or reason can be drawn from this crazy quilt of case law. The self-critical evaluation privilege is of recent origin and one that is narrowly applied even in those jurisdictions where it is recognized. On their own, the cases give some indication what one may expect in a particular jurisdiction, but because of the lack of well-settled precedents, it is equally feasible to expect that a court could refine its thinking with proper persuasion. Counsel who seek to invoke the self-critical analysis privilege should apply the principles of *Shipes*, *Ashley*, *Roberts* and *Lawson* in their arguments to emphasize and distinguish the test to be applied.

Perhaps the most significant barrier occurs when a court disagrees that voluntary self-critical analysis will be abandoned if it is later found to be discoverable in litigation. The *Dowling* court asserted:

> Organizations have many incentives to

42. 191 F.R.D. at 386.

> conduct such reviews that outweigh the harm that might result from disclosure. The most prominent of these is surely the desire to avoid law suits arising from unsafe conditions. But organizations also have a strong incentive to [seek] . . . a reputation for safety [that] renders a product more marketable.[43]

Even if true, is this enough to justify prohibiting an enterprise the benefit of the self-critical analysis privilege and withholding from the public the benefit of encouraging self-improvement through uninhibited self-analysis and evaluation?

B. Evidence Rules

All the cases discussed above were decided based on state evidence laws consistent with Rule 501 of the Federal Rules of Evidence or under Rule 501 itself. Rule 501, the general rule governing privileges, recognizes no particular privilege; it encourages a case-by-case consideration. The privilege of self-critical analysis, as a product of Rule 501, could protect a self-critical document from both discovery and later use at trial. Yet even if the state choose reasonable criteria or tests by which to measure the application of the privilege and applied them fairly, the result would be still a patchwork of local law.

The U.S. Supreme Court stated in *Trammel* that it will not create and apply an evidentiary privilege unless it "promotes sufficiently important interests to outweigh the need for probative evidence, [and as] . . . testimonial exclusionary rules and privileges contravene the fundamental principle that 'the public . . . has a right to every man's evidence,'" any such privilege must "be strictly construed."[44]

Moreover, although Rule 501 manifests a congressional desire "not to freeze the law of privilege," but rather to provide the courts with flexibility to develop rules of privilege on a case-by-case basis, according to *Trammel*, the Supreme Court has expressed no interest in exercising this authority expansively. The Court opined that the balancing of conflicting interests of this type is particularly a legislative function.

On the other hand, although Rule 407 may be a limited evidentiary shield, the policy behind it of limiting admissibility of remedial measures as proof of negligence or culpable conduct is consistent with the privilege claimed under self-critical analysis. Rule 407, entitled "Subsequent Remedial Measures," states:

> When, after an injury or harm allegedly caused by an event, measures are taken that, if taken previously, would have made the injury or harm less likely to occur, evidence of the subsequent measures is not admissible to prove negligence, culpable conduct, a defect in a product, a defect in a product's design, or a need for a warning or instruction. . . .[45]

Federal courts that have applied this rationale are split as to its import. The District Court of Minnesota recognized Rule 407 as a rule of public policy rather than one of relevancy, but questioned its applicability to matters of pretrial discovery.[46] On the contrary, the Northern District of Florida relied on Rule 407 in its decision recognizing the self-evaluative privilege to protect environmental audits.[47]

Strong support therefore exists for the view that the self-evaluative privilege should be analyzed under the subsequent remedial measures rationale of Rule 407 rather than the "relational privileges" protected under Rule 501. In this focus, self-evaluative practices within an organization would be seen more sensibly as remedial measures, rather than activities involving the kind of confidential relationships that Rule 501 seeks to protect.

Courts that have upheld the self-evaluative privilege did not limit discovery of factual matters, only the self-evaluations

---

43. 971 F.2d at 426.

44. 445 U.S. at 50, 51, *quoting* United States v. Bryan, 339 U.S. 323, 331 (1950).

45. The Advisory Committee's Note to Rule 407 clarifies that courts have applied the principle broadly to exclude "evidence of subsequent remedial repairs, installation of safety devices, changes in company rules, and discharge of employees."

46. Capellupo v. FMC Corp., 1988 U.S.Dist. Lexis 3792 (D. Minn. 1989). *See also* 2 WEINSTEIN, EVIDENCE ¶ 407[07], at 407-37 through 407-38.

47. Reichhold, 157 F.R.D. at 524.

and their related conclusions and actions. This result is quite similar to that which would be achieved under a Rule 407 analysis. As Judge Posner of the Seventh Circuit has stated, the major purpose of Rule 407 "is to promote safety by removing the disincentive to make repairs (or take other safety measures) after an accident that would exist if the accident victim could use those measures as evidence of the defendant's liability."[48]

A GOOD RESULT

The implications of this shift in analysis are significant. The primary ramification is that the self-evaluative privilege would apply not against the initial discovery request, but rather as a bar against admission of the evidence at trial. This would allow discovery of the facts of the self-evaluative evidence, consistent with the holdings of the federal courts, which support the privilege, but the analysis and any remedial measures themselves could not be introduced at trial as evidence of negligence or culpability.

Therefore, it is recommended that an argument based on Rule 407 should be included with an argument grounded in Rule 501 in any judicial review of the applicability of the privilege, or any legislative effort to codify the privilege.

48. Flaminio v. Honda Motor Co., 733 F.2d 463, 469 (7th Cir. 1984).

The Privacy Project

Cybersmear May Be Coming to a Website Near You: A Primer for Corporate Victims

How to respond or combat venomous comments from current or former disgruntled employees presents both legal and non-legal problems

By Thomas G. Ciarlone Jr. and Eric W. Wiechmann

SAMUEL Taylor Coleridge wrote, "Whispering tongues can poison truth." The Internet is no exception to this simple maxim. With one of three Americans logging onto it daily, and at least 350 million users worldwide by 2003, the Internet has the potential to become the electronic rumor mill for the new millennium.[1]

Much of the time, online gossip is merely scurrilous and perhaps embarrassing. For example, corporate executives and their alleged sexual proclivities are favorite topics for online badmouths.[2] Sometimes, however, boorish banter gives way to injurious falsehood. Consider the story of popular cookie manufacturer Mrs. Fields. In 1996, speeding along the information superhighway was speculation that the company planned to donate pounds of cookies, brownies and other sweets to an O.J. Simpson victory party. Despite its facial implausibility, this myth inspired rumblings of a national boycott. Mrs. Fields was unable to expose the hoax until it retained a public relations firm at great expense.[3]

IADC member Eric W. Wiechmann is a litigation partner of Cummings & Lockwood, LLC, in the firm's Harford, Connecticut, office. He is a graduate of Hamilton College (B.A. 1970) and Cornell Law School (J.D. 1974).

A litigation associate in the firm's Stamford, Connecticut, office, Thomas G. Ciarlone Jr. was educated at New York University (B.A. 1998) and Cornell Law School (J.D. 2001).

Then there is Varian Medical Systems, a publicly traded, Fortune 500 company with a market capitalization in the billions. Disgruntled former employees posted more than 14,000 messages—on hundreds of websites—accusing the company and its management of everything from homophobia to pregnancy discrimination to the surreptitious videotaping of public bathrooms. When Varian sued them for defamation, the defendants turned around and created their own web site. Varian prevailed on the merits after a protracted trial.[4] But as a practical matter, it may have won the battle but lost the war. It incurred substantial legal fees and generated negative publicity,

1. *See Drilling Down into Computer and Web Trends*, at http://www.learnframe.com/aboutelearning/page16.asp; Bruce W. Sanford & Michael J. Lorenger, *Teaching an Old Dog New Tricks: The First Amendment in an Online World*, 28 CONN. L. REV. 1137, 1137 (1996); Geoff Thompson, *$40,000 Awarded in First Cyberspace Defamation Case*, AUSTRALIAN FIN. REV., May 4, 1994, at S41 ("uninhibited defamation is one of the things that makes cyberspace such a fun place to be").

2. *See, e.g., Cybersmear Litigation Joins Online Arsenal Ridge*, THE RECORD, March 1, 2000, at B01, available at 2000 WL 15812270.

3. *Liar, Liar: Unscrupulous Web Pages*, PC COMPUTING, December 1, 1998, at 89.

4. Shannon Lafferty, *California Internet Libel Suit Yields Big Verdict*, THE RECORDER [San Francisco], December 14, 2001, available in archive at www.law.com/california.

but it has yet to silence the defendants, who continue to lambaste the company on their home page. The victory was bittersweet and more or less pyrrhic.[5]

As a general proposition, civil libertarians would applaud this result. These activists insist that the typical action to suppress online discourse is frivolous. It serves only to harass, they say, and often offends constitutional rights, including those to privacy and free speech.[6]

Taken to its extreme, this rhetoric brings David and Goliath into the digital age: Corporations dig deep into their pockets to pay for lawyers whose tactics aim to intimidate and ultimately muzzle computer-savvy but underfinanced critics.[7] Whatever facial appeal it may have, such hyperbole cannot withstand closer scrutiny. To urge that corporate America seeks only retribution when it pursues scandalmongers is to ignore certain economic realities and policy concerns.

When broadcast over the Internet, defamatory speech sometimes causes substantial monetary losses, especially for publicly traded companies. Stock prices can fluctuate wildly; their movement is a function of information or, as the case may be, misinformation. Cyberlibel can manifest itself not only as personal potshots that bruise egos, but also as institutional slurs that move markets. Companies that try to curb the dissemination of misinformation are improperly cast as corporate bullies. Quite the contrary. These companies are honoring their obligation to shareholders to attend to matters that jeopardize reputation, brand name, and thus profitability.[8]

Unbridled innuendo has broader, systemically corrosive consequences to society. It compromises meaningful dialogue. Cloaked in anonymity and unencumbered by editorial filters, almost anyone with a computer can take to the Internet and share their convictions with the world at large. This has the cumulative effect of generating massive amounts of conflicting information, the credibility of which is frequently beyond evaluation. The online marketplace of ideas becomes increasingly incoherent and in the final analysis struggles to fulfill what should be its central role: an arena in which competing ideas collide, but out of which the truth eventually emerges.

What are the theories of liability that corporate plaintiffs may enlist to combat cybersmear campaigns? What are the pros and cons of bringing suit? What are the alternatives to litigation? What preventive measures are there to reduce both the incidence and the impact of digital defamation?

THEORIES OF LIABILITY

While purveyors of fibbery are sued time and again for defamation, other causes of action can lie against them. Depending on the facts, they might be prosecuted for, among other things, violating securities laws, breaching contracts, or diluting intellectual property. In any event, affected businesses should appreciate that their options are not necessarily limited to classic theories of defamation.

---

5. *See* the following stories, all in THE RECORDER by Shannon Lafferty and all available in archive at www.law.com/california: *Defendants Not Nice in Internet Case*, November 6, 2001; *No Easy Outs Seen in Suit for Internet Libel*, December 12, 2001; *Judge Silences Ravings of Angry Ex-employees*, December 13, 2001; *Web War of Words Drawing More Hits*, March 26, 2002; *Contempt Hearing Set in Internet Libel Case*, March 27, 2002; *Court Issues Stay in Case over Web Defamation*, April 18, 2002; *FBI Investigating Death Threats in Varian Libel Case*, August 1, 2002. *See also* www.geocities.com/mobeta_inc/slapp/slapp.html.

6. *See generally* Joshua R. Furman (Comment), *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does As Strategic Lawsuits Against Public Participation*, 25 SEATTLE U.L. REV. 213 (2001); Bruce P. Smith, *Cybersmearing and the Problem of Anonymous Online Speech*, COMM. LAW. 3 (18-Fall 2000).

7. *See, e.g.*, Jeffrey R. Elkin, *Cybersmears: The Next Generation*, 10 BUS. L. TODAY 42 (August 2001).

8. *See generally* Werner F.M. De Bondt & Richard H. Thaler, *Does the Stock Market Overreact?* 40 J. FIN. 793 (1985); Wayne Joerding, *Are Stock Prices Excessively Sensitive to Current Information?* 9 J. ECON. BEHAV. & ORG. 71 (1988); Mark J. Roe, *The Shareholder Wealth Maximization Norm and Industrial Organization*, 149 U. PA. L. REV. 2063, 2065.

A. Defamation

1. Libel or Slander

There is a dearth of precedent as to whether electronic communications are subject to the rules of libel, on the one hand, or of slander, on the other. Doctrinally, this issue turns—obviously enough—on whether such communications are more analogous to the printed or the spoken word.

The same issue confronted the legal community when radio and television first became popular. Initially, when broadcasters read from scripts, libel provided the rule of law, but when they spoke extemporaneously, slander principles applied.[9] Over time, courts "recognized the breadth of exposure and resulting damage from broadcast defamation was akin to published defamation, and began to apply libel standards to broadcast defamation."[10] Today television stations are considered publishers of libelous material, with limited exceptions to this rule,[11] notwithstanding any absence of a script.[12] To the extent that the Internet is susceptible to classification, it has evolved into an interactive blend of print and broadcast media.[13] Courts should be expected to invoke libel, as opposed to slander, in online defamation cases.[14]

This observation is hardly just an academic one. It has practical and, for that matter, positive ramifications for corporate victims of cybersmear. At common law, a prima facie case of slander requires a greater quantum of proof. In particular, the slander plaintiff must demonstrate that which the libel plaintiff need not: special damages, as distinguished from actual or general damages, or, stated differently, actual pecuniary harm.[15]

In a libel action, that is to say, plaintiffs must establish only injury to reputation; they need not go a step further and prove resultant economic damages. The underlying rationale is that the relative permanence of the written word raises a presumption of harm, whereas the ephemeral qualities of speech cannot occasion a similar inference.

Modern jurisprudence, however, is in some instances collapsing the distinction between libel and slander. As a result, some states—most notably, New York—have begun to require proof of special damages even when libel is the theory on which suit has been brought.[16]

---

9. LAURENCE H. ELDREDGE, THE LAW OF DEFAMATION § 13, at 83 (1978).

10. Anthony M. Townsend et al., *Libel and Slander on the Internet*, 43 COMM. OF THE ACM 15, 15-17 (June 2000).

11. California, for example, still adheres to the minority view, treating defamatory statements on television and radio as slander. *See generally* CAL. CIV. CODE ANN. §§ 46, 48.5; Arno v. Stewart, 54 Cal.Rptr. 382 (Cal.App. 1966).

12. *See* Finley P. Maxson (Note), *A Pothole in the Information Superhighway: BBS Operator Liability for Defamatory Statements*, 75 WASH. U. L.Q. 673, 676 n.13 (1997).

13. *See, e.g.*, Julie Adams, *Will Wage Gap Persist for Women in New Media?* in Harvard Third Biennial Conference on Internet & Society, available at www.news.harvard.edu/net_news2000/06.02/wage.html (last updated June 2, 2000).

14. But some commentators suspect otherwise, predicting that slander laws may ultimately control certain iterations of online defamation. *See, e.g.*, Karen S. Frank, *Potential Liability on the Internet*, 437 PLI/Pat. 417, 437 (1996).

15. *See, e.g.*, Vanover v. Kansas City Life Ins. Co., 553 N.W.2d 192, 197 (N.D. 1996); Stickle v. Trimmer, 143 A.2d 1, 3 (N.J.Super. 1958), *cert. denied*, 145 A.2d 168 (N.J. 1958). *See also* Susan Oliver, *Opening the Channels of Communication among Employers: Can Employers Discard Their "No Comment" and Neutral Job Reference Policies?* 33 VAL. U. L. REV. 687, 700 (1999) (harm or actual injury presumed with written defamatory statements because written statements are likely to be permanent; slander plaintiff must prove special harm or actual pecuniary loss). *Accord* ELDREDGE, *supra* note 9, § 12, at 77; DAN B. DOBBS, THE LAW OF TORTS § 409, at 1144.

See also RESTATEMENT (SECOND) OF TORTS § 569 (1977) ("One who falsely publishes matter defamatory of another in such a manner as to make the publication a libel is subject to liability to the other although no special harm results from the publication.")

16. *See, e.g.*, Boule v. Hutton, 138 F.Supp.2d 491, 506 (S.D. N.Y. 2001) (applying New York law). But inasmuch as it muddies the doctrinal waters of defamation, this trend has been the target of some criticism. *See, e.g.*, Mike Steenson, *Defamation Per Se: Defamation By Mistake?* 27 WM. MITCHELL L. REV. 779, 809 (2000).

Legal philosophy aside, the bottom line is clear: if cast in the role of defamation plaintiff, a corporation, whenever possible, should proceed under a theory of libel rather than slander. While in the final analysis the former may prove only marginally easier to maintain, common sense alone dictates that no advantage go unexploited.

2. Libel Defenses

Even though special damages are often not a prerequisite to recovery, libel remains a notoriously difficult cause of action to prosecute successfully,[17] not because of a high prima facie hurdle, but because of a panoply of privileges and affirmative defenses that do not lend themselves to refutation.[18] Figuring most prominently among them is, of course, the First Amendment.

a. Constitutional Privileges

(i) Opinion

Opinions are tantamount to ideas, the policing of which is rightly the province of neither judges nor juries. Opinions are often not actionable under a theory of libel,[19] but the U.S. Supreme Court has stressed that its decisions have stopped short of carving out a wholesale defamation exemption for "opinion."[20] Indeed, to the extent it serves as a defense to libel, opinion is narrowly defined and reaches only statements that cannot be proved false or that cannot be reasonably interpreted as stating actual facts about an individual.[21]

Because of this closely circumscribed definition, accused libelists cannot escape liability by qualifying their defamatory utterances with the caveat that they were merely expressing opinions, rather than statements of fact. Accepting such superficial assurances at face value would elevate form over substance in an flourish of naïveté.[22] As the First Circuit has put it, "to say 'I think' is not enough to turn fact into opinion, where what is supposedly 'thought' is, or implies, a proposition of fact."[23]

The question becomes: Under what circumstances will a statement, however unflattering, find refuge under cover of opinion? Because libel cases are almost invariably fact-intensive, a satisfying answer is difficult to come by. One federal judge has ventured that a statement takes on the character of opinion "where it involves expressions of personal judgment, especially as the judgments become more vague and subjective in character."[24]

In effect, courts subscribe to that kernel of wisdom first inspired by bullies and hatched in playgrounds: "Sticks and stones may break my bones, but names will never hurt me." While the adage is a simple one,

---

17. *See, e.g.*, Bonheur v. Dresdner Bank, 1986 WL 4702, at *2 n.2 (S.D. N.Y.); Lyrissa Barnett Lidsky, *Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It*, 73 TUL. L. REV. 173, 198 n.103 (1998). When set against the backdrop of the Internet, libel is further complicated by a host of knotty, extralegal concerns.

18. *See, e.g.*, Robert E. Drechsel, *The Paradox of Professionalism: Journalism and Malpractice*, 23 U. ARK. LITTLE ROCK L. REV. 181, 194-95 (2000); James C. Goodale & Rex S. Heinke, *Libel Litigation: Summary Judgment*, 338 PLI/Pat. 137, 139 (1992); Kevin T. Peters, *Defamation and the First Amendment: Recent Cases Emphasizing the Content of Defamatory Communications and the Nature of the Communicator*, 20 SUFFOLK U. L. REV. 1089, 1092 (1986).

19. Gertz v. Robert Welch Inc., 418 U.S. 323, 339-40 (1974), *rev'g and remanding* 471 F.2d 801 (7th Cir. 1072); Henry v. Nat'l Ass'n of Air Traffic Specialists Inc., 836 F.Supp. 1204, 1214 (D. Md. 1993); Gifford v. Nat'l Enquirer Inc., 1993 WL 767192, at *5 (C.D. Cal.); Davis v. Ross, 754 F.2d 80, 85 (2d Cir. 1985); Hotchner v. Castillo-Puche, 551 F.2d 910, 913 (2d Cir. 1977), *cert. denied*, 434 U.S. 834 (1977)).

20. Milkovich v. Lorain Journal Co., 497 U.S. 1, 18 (1990), *rev'g and remanding* 545 N.E.2d 1320 (Ohio App. 1989).

21. *See generally* Philadelphia Newspapers Inc. v. Hepps, 475 U.S. 767 (1986), *rev'g and remanding* 485 A.2d 374 (Pa. 1984); Greenbelt Coop. Pub. Ass'n v. Bresler, 398 U.S. 6 (1970), *rev'g and remanding* 252 A.2d 755 (Md. 1969); Old Dominion Branch No. 469, Nat'l Ass'n of Letter Carriers v. Austin, 418 U.S. 264 (1974), *rev'g* 192 S.E.2d 737 (Va. 1972); Hustler Magazine Inc. v. Falwell, 485 U.S. 46 (1988), *rev'g* 797 F.2d 1270 (4th Cir. 1986); Milkovich, 497 U.S. 19.

22. Cianci v. New Times Pub. Co., 639 F.2d 54, 64 (2d Cir. 1980)

23. Gray v. St. Martin's Press Inc., 221 F.3d 243, 248 (1st Cir. 2000) (citations omitted).

24. *Id.* at 248.

subsumed under it is an important lesson: Corporate managers must recognize the difference between the truly pestilent and the merely vulgar and indecorous—the stuff that batters big egos, rather than big profits. Legal action properly presents itself as an option only with respect to the former genus of online opprobrium.

(ii) Parody

Satire is everywhere, and perhaps due in part to its prevalence, it frequently lies outside the bounds of actionable defamation. "There is no libel," according to one appellate court, where the "material is susceptible of only non-defamatory meaning and is clearly understood as being parody [or] satire."[25] That is not to say, however, that the comedian enjoys a license to defame.

What sets parody apart from other strains of humor is its essential character, one of conspicuous "distortion and exaggeration. [L]ike the warped and curved mirrors in a carnival fun house, it depends upon the grotesque for its effects."[26] Stated differently, parody can be mistaken for nothing else, and its satirical nature is immediately self-evident. For that reason, a parody necessarily cannot "defame . . . by false attribution or presentation of false facts."[27]

Corporate executives must recognize that they and their companies may become fodder for satirists whose work appears on web pages, in discussion groups, or in chat rooms. This bothersome reality is best viewed as a cost of doing business, rather than a reason to retain counsel. Although it is frustrating to be the butt of a joke built on hyperbole or tall talk, the law simply offers little relief to those whose only complaint is that they have been reduced to caricatures.

(iii) Public Figures

Commenting on the debate surrounding the highly publicized shootings of four teenagers in a Manhattan subway, a New York judge opined that it "is a paramount interest of a free society to assure that open and spirited discussion of matters of public concern will not be chilled by the threat of litigation."[28] Such unabashed endorsement of the marketplace of ideas harkens back to a landmark decision of the U.S. Supreme Court, *New York Times Co. v Sullivan*,[29] in which the Court held that public officials and figures may recover for defamatory statements only when the statements are made with "actual malice"—that is, with knowledge of their falsity, or with reckless disregard for the truth.

Defining who are public figure, however, is no easy task. At the risk of oversimplification, it may be said that public figures typically hail from one of two factions: those who "occupy positions of such persuasive power and influence that they are deemed public figures for all purposes" or those who "have thrust themselves to the forefront of particular public controversies in order to influence the resolution of the issues involved."[30]

Examples of the sorts of personalities that courts have classified as public figures include political activists, candidates for office and even football coaches who become state university athletic directors.[31] Natural extensions of these examples would include executives at major corporations who become ensnarled in controversies implicating matters of public concern. Take, for instance, Bill Gates, founder of software giant Microsoft. His antitrust debacle with the Justice Department has transformed him into the archetypal public figure, perhaps explaining why he has become a favorite subject for editorial car-

---

25. Salek v. Passaic Collegiate Sch., 605 A.2d 276, 278 (N.J.Super. 1992), *citing* Romaine v. Kallinger, 537 A.2d 284, 288 (N.J. 1988).

26. Salomone v. MacMillan Pub. Co., 411 N.Y.S.2d 105, 109 (Sup.Ct. N.Y. County 1978).

27. *See, e.g.*, San Francisco Bay Guardian Inc. v. Superior Ct. (Sparks), 21 Cal.Rptr.2d 464, 467 (Cal.App. 1993).

28. Goetz v. Kunstler, 625 N.Y.S.2d 447, 453 (Sup.Ct. N.Y. County 1985).

29. 376 U.S. 254 (1964).

30. Gertz, 418 U.S. at 345.

31. *See generally* Curtis Pub. Co. v. Butts, 388 U.S. 130 (1967), *aff'g* 351 F.2d 702 (5th Cir. 1965); Monitor Patriot Co. v. Roy, 401 U.S. 265 (1971), *rev'g and remanding* 254 A.2d 832 (N.H. 1969).

toonists whose works are scattered far and wide across the Internet.

Gates—or, for that matter, anyone similarly situated—could proceed against his critics only with great difficulty, since they could almost certainly avail themselves of the heightened actual malice standard. Perhaps more important, for a public figure to initiate a libel action is often to ignite a public relations nightmare.

Besides, litigation is not necessarily the most effective solution for a prominent persona. Abraham Lincoln said that "truth is generally the best vindication against slander." In this respect, "public figures usually enjoy significantly greater access to the channels of effective communication and hence have a more realistic opportunity to counteract false statements then private individuals normally enjoy."[32] Since both the courts and the public at large are keenly aware of this imbalance in power, the corporate behemoth that accuses a single, vociferous individual of defamation may appear to be using the law not as an instrument of justice, but instead as a tool of coercion.

2. Common Law and Statutory Defenses

a. Anti-SLAPP Legislation

Home to Silicon Valley and its hotbed of Internet start-ups, California has erected a heightened barrier to recovery for online defamation—the Strategic Lawsuit Against Public Participation Act, conveniently known by the acronym SLAPP.[33] On a legislative finding that "a disturbing increase in lawsuits brought primarily to chill the valid exercise of the constitutional right of freedom of speech," the legislation requires libel plaintiffs to establish a likelihood of success on the merits before trial. Should they fail to make this showing, they subject their defamation claims to a special motion to strike, which generally will succeed if the challenged statements amount to acts in furtherance of the right of "petition or free speech," which are defined as, among other things, "statement[s] or writing[s] made in a place open to the public or a public forum in connection with . . . issue[s] of public interest."

Referring to this language, a California appellate court ruled that Internet discussion groups about the management of publicly held companies are "open and free to anyone who wants to read" them, are relevant to matters of public interest, and are thus "public forums" for purposes of the legislation. The court then recognized a range of comments from one such discussion group as "disparaging" but nonetheless non-actionable.[34]

At least a dozen other jurisdictions—including New York, Massachusetts and Florida—have enacted similar statutory schemes.[35] Legislators have not ignored the public perception that, through predatory litigation tactics, big business sometimes exploits the power and resources it has. Before dragging cyberlibelists into court, large corporate entities should be certain that their claims are not just legally cognizable, but also are compelling, persuasive and meritorious. Otherwise, libel defendants may reach up their sleeves for an

---

32. Gertz, 418 U.S. at 344.

33. CAL. CIV. PROC. CODE § 425.16.

34. ComputerXpress Inc. v. Jackson, 113 Cal. Rptr.2d 625 (Cal.App. 2001) (company became matter of public interest merely because it was "publicly traded company" and "had inserted itself into the public arena by means of numerous press releases"). The posted comments were far from innocuous and included the abrasive likes of the following: "When the people who have . . . been duped into this stock realize the scam they were coaxed into, my guess is there will be hell to pay."

35. DEL. CODE ANN. tit. 10, §§ 8136-8138 (Supp. 1996); FLA STAT. ANN. § 768.295 (West 2000); GA. CODE ANN. § 9-11-11.1 (Supp. 1997); IND. CODE ANN. §§ 34-7-7-1 to 34-7-7-10 (West Supp. 1998); LA. CODE CIV. PROC. ANN. art. 971 (West 1999); ME. REV. STAT. ANN. tit. 14, § 556 (West Supp. 1997); MASS. GEN. LAWS ANN. ch. 231, § 59H (West 1997); MINN. STAT. ANN. §§ 554.01-554.05 (West Supp. 1997); NEB. REV. STAT. §§ 25-21,241 to 25-21,246 (1995); NEV. REV. STAT.. §§ 41.640-41.670 (Supp. 1993); N.Y. C.P.L.R. § 3211(g) (McKinney 1997-1998); OKLA. STAT. ANN. tit. 12, § 1443.1 (1999); R.I. GEN. LAWS §§ 9-33-1 to 9-33-4 (Supp. 1996); TENN. CODE ANN. §§ 4-21-1001 to 4-21-1003 (1997); WASH. REV. CODE ANN. §§ 4.24.500-4.24.520 (West Supp. 1997).

anti-SLAPP statute, use it to cast themselves in the role of David and garner the sympathy that courts often afford the underdog.

b. Retraction Statutes

Ordinarily, the public retraction of a libelous statement does not defuse liability but does mitigate damages.[36] While historically a function of common law, this principle today is embedded in so-called "retraction statutes," which provide that the timely renunciation of defamatory declarations will serve to limit damages, usually to those for actual harm.[37]

For purposes of online defamation, however, retraction statutes may offer little or no shelter to average defendants, who often are individuals, acting alone or in collaboration with a few friends, and who spread their word on electronic bulletin boards, in Internet chat rooms and on independent web sites. Retraction statutes typically reach members of the media, to the exclusion of all other classes of libel defendants.[38]

A widely cited decision from the Wisconsin Court of Appeals illustrates this. In *It's in the Cards Inc. v. Fuschetto*,[39] the court held that a trial judge had erred by granting summary judgment to the defendant, on the grounds that the plaintiffs had never demanded a retraction pursuant to a state statute. Rosario Fuschetto, the defendant, had made a series of allegedly defamatory statements about the plaintiffs, a sports memorabilia store and its owner. Fuschetto posted his statements on an electronic bulletin board to which a community of subscribers had open access. The court held that the Wisconsin retraction statute did not apply to bulletin board postings because they do not constitute a "publication" according to its ordinary meaning.

In the end, corporate victims of cybersmear, if they elect to pursue their harassers in court, usually can dispense with concerns over retraction statutes—at least with respect to the merits of their cases. Even when retraction laws are facially inapplicable to non-media defendants, badmouths who voluntarily forswear their words still can insulate themselves from liability, albeit not completely, because, however motivated, retractions will tend to breed evidence of good faith and thus mitigate damages.[40]

c. Statutes of Limitations

The limitations period for a libel claim customarily begins to run upon the publication of the purportedly libelous material. Establishing the date of publication for libel appearing in a book, newspaper or magazine is a relatively straightforward task. The same cannot be said of libel that manifests itself on the Internet.

The dynamic nature of the online community is to blame—or, as some may see it, credited—for this difficulty. Unlike those memorialized on paper and in ink, messages broadcast on the Internet can propagate at truly exponential rates. This robust proliferation is attributable to a variety of causes, so-called "hypertext" perhaps the most prominent among them.

Hypertext lies at the heart of the Internet and the programming language—hypertext

---

36. *See, e.g.*, ROBERT D. SACK. LIBEL, SLANDER AND RELATED PROBLEMS § V.5.1.1 at 211 (1980).

37. *See, e.g.*, CONN. GEN. STAT. ANN. § 52-237 (West 2002); NEB. REV. STAT. § 25-840.01 (2001). Some jurisdictions go so far as to make a request for retraction a condition precedent to filing a libel suit. FLA. STAT. ANN. § 770.01 (West 2001).

38. In Hinerman v. Daily Gazette Co., 423 S.E.2d 560, 595 n.21 (W.Va. 1992), Miller, J., dissenting, noted different statutes and stated: "California, for example, follows the majority approach and provides only for certain media defendants in its retraction statute, while Connecticut, Louisiana, Maine, Massachusetts, Nebraska, Texas, and West Virginia apply their statutes to all defendants."

39. 535 N.W.2d 11 (Wis.App. 1995).

40. Jonathan D. Hart et al., *Cyberspace Liability*, 523 PLI/Pat. 123, 163 (1998).

41. Matisse Enzer, *Glossary of Internet Terms*, available at www.matisse.net/files/glossary.html#H (updated February 24, 2002). See also www.netdictionary.com/html/h/html, which defines html as "[t]ext that includes links or shortcuts to other documents, allowing the reader to easily jump from one text to related texts, and consequentially from one idea to another, in a non-linear fashion."

markup language, commonly referred to as HTML—that gives it interactive life. At the risk of oversimplifying matters, hypertext has been defined as "any text that contains links to other documents—words or phrases in the document that can be chosen by a reader and which cause another document to be retrieved and displayed."[41] Since ramping onto the Internet has become an inexpensive proposition, the likes of hypertext and the complex network of interconnectivity that it inspires can transform a person's keystrokes into gospel for the masses.

Aside from its practical implications, hypertext raises jurisprudential concerns over the time at which claims for cyberlibel accrue. "Under the single publication rule," one commentator has written, "a cause of action accrues at the time of the original publication; therefore, subsequent shipments and . . . reprintings of the same edition of the work do not extend the date." But, at the same time, "reprintings of a book in a new edition . . . will usually constitute a new publication of the libel."[42]

While application of these rules is simple enough for print media, their extension to the digital frontier is awkward. The fundamental nature of the World Wide Web—and the billions, if not trillions, of hypertextual links populating it—blur the distinctions between reprinting and subsequent editions. To date, the courts have offered next to no guidance on this issue. While this is sure to change over time, libel plaintiffs must for the moment arm themselves only with the knowledge that defenses based on limitations periods may present issues of first impression that require creative argumentation rather than extensive reliance on existing precedent.

d. Insulated ISP

Deep corporate pockets are on the short list of defendants in just about any tort action. Libel claims are no different. Unlike print media giants, however, Internet heavyweights can often find asylum from defamation in a unique array of defenses. In this way, libel plaintiffs inevitably face uphill, if not impossible, battles when matched against the likes of America Online, Yahoo! and other web portals and internet service providers (ISPs).

Among the most potent of these defenses is the Communications Decency Act of 1996 (CDA), 47 U.S.C. § 230 *et seq.* Enacted to overrule a decision of a New York trial court,[43] the CDA states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This Good Samaritan provision, as it is frequently called, has been construed to largely immunize the ISP industry against defamation lawsuits.

In *Zeran v. America Online Inc.*,[44] for example, a Virginia federal district court refused to hold America Online (AOL), the largest ISP in the United States, accountable for a series of profoundly distasteful messages that one of its users had posted to an AOL bulletin board. The messages advertised tee shirts containing slogans that joked about the 1995 bombing of the federal building in Oklahoma City. Worst of all, the name and telephone number of the plaintiff, Zeran, were included in the messages, although he had absolutely nothing to do with them. He was inundated with a barrage of harassing telephone calls, a number of them threatening his life.

Alleging that it failed to take timely steps to delete the messages and to cancel the account of the offending user, the plaintiff sued AOL for his monetary loss and emotional suffering. Laboring under the express terms of the CDA, the district court was all but obligated to reject his claim pursuant to a theory of statutory immunity.

The legal hurdles to prosecuting an ISP

---

42. Elizabeth A. McNamara, *A Selective Survey of Current Issues Facing Book and Magazine Publishers*, 601 PLI/Pat. 9, at 45 (2000).

43. Stratton-Oakmont Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup.Ct. Nassau County) (defendant liable for statements that one of its subscribers posted on electronic message board over which it exercised some editorial control).

44. 958 F.Supp. 1124 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997).

for the defamatory remarks of its users carry dire consequences for the cyberlibel plaintiff. Because of the inherently anonymous character of the Internet, to try to identify an online defamer may be to attempt the impossible.[45] So with ISPs shrouded in statutory protections and libelists cloaked in anonymity, parties aggrieved by cybersmear may be left with fingers, but with nowhere to point them.

B. Collateral Theories of Liability

Although defamation is the most obvious theory on which cybersmear plaintiffs may rely, creative litigants can sometimes turn to other causes of action in their pursuit of online irritants. In this realm, however, the law is in the throes of infancy and thus remains a necessarily scant and often unsettled lot.

1. Employment Relationship

Unhappy, disgruntled current and former employees comprise a common class of cyberlibelists.[46] Armed with inside information, office gossip and axes to grind, they have used the Internet to launch attacks against corporate entities big and small. Sometimes, these offensives are not defamatory but are in derogation of contracts attendant to the employment relationship.

The execution of a confidentiality or nondisclosure agreement is becoming an increasingly standard term of employment, especially in high-tech industries.[47] When drafted broadly enough, they can endow employers with an instrument to silence detractors who are a drain on more than just their payrolls. Of course, shrewd employees—versed in the contractual prohibitions to which they are subject—can skirt the edges of confidentiality agreements, for instance, by carefully eschewing references to trade secrets, proprietary data and related varieties of sensitive information.

Dissatisfied employees who grumble, gripe and grouse over the Internet also may violate provisions embedded in employment manuals or other internal company policies. Several legal commentators have alluded to this possibility,[48] which presumably would at a minimum help justify the discharge of refractory employees.

2. Securities Laws and Business Torts

Transmitted via the Internet, false or otherwise misleading reports about a company, especially those opining on its financial stead or its business prospects, can wreak immediate and sometimes irreversible havoc. When this happens, affected companies should look beyond defamation law to vindicate their rights. In *Hart v. Internet Wire Inc.*,[49] for example, a former employee of the defendant news wire concocted a phony press release about Emulex Corp. After short selling large blocks of Emulex stock, he sent the release to Internet Wire, which then published it. The bogus release subsequently was redistributed by Bloomberg News, another but much larger news service. Predictably, the price of Emulex stock plunged to $60 a share in just 15 minutes.

The plaintiff sued under color of federal law, alleging that both Bloomberg and Internet Wire had run afoul of Section 10(b)(5) of the Securities Exchange Act of

---

45. *See* Nancy Toross (Note), *Double-Click on This: Keeping Pace with On-Line Market Manipulation*, 32 LOY. L.A. L. REV. 1399, 1419 (1999) (one can "hide his or her identity on the Internet and make statements on an anonymous or false basis, thus making it difficult to identify and prosecute"); Shahram A. Shayesteh (Comment), *High-Speed Chase on the Internet Superhighway: The Evolution of Criminal Liability for Internet Piracy*, 33 LOY. L.A. L. REV. 183, 193-94 (1999) (discussing various means by which Internet users can hide their true identities).

46. *See, e.g.*, Peter Schnitzler, *Web Attacks Tough to Stop*, INDIANAPOLIS BUS. J., May 6, 2002, at 19; Stephanie Armour, *Courts Frown on Online Badmouthing; Grousing Ex-workers Lose Legal Battles*, USA TODAY, January 7, 2002, at B01.

47. *See, e.g.*, Carole Levitt, *Computer Counselor*, L.A. LAWYER, October 2000, at 62.

48. *See, e.g.*, Tonianne Florentino, *Privacy in the Ever-evolving Workplace*, 632A PLI/Pat. 453, 463-65 (2001).

49. 145 F.Supp.2d 360 (S.D. N.Y. 2001).

1934. Although the plaintiff later succumbed to a motion to dismiss, his claim failed only because neither defendant had published the fictitious press release with the requisite scienter—that is, an intent to defraud or with fraudulent intent.

Under slightly different facts, in other words, the plaintiff could have successfully prosecuted his 10(b)(5) claim. In fact, recognizing the vast potential for the manipulation of stock prices through online embroidery, the Securities and Exchange Commission has established an Office of Internet Enforcement, which employs about 60 attorneys "who devote substantially all of their time to [the] detection and investigation of fraud on the Internet."[50] The plaintiff might also have brought a derivative action against the author of the press release for, among other things, commercial disparagement, sometimes known as trade libel,[51] and tortious interference with business relations.

So, while it may generally be the most apposite, libel is not necessarily the only theory of liability that can ensnare digital defamers.

3. Intellectual Property

When corporations are derided online, their intellectual property is frequently implicated. Often, their trademarks are coopted, inextricably entwined in defamatory speech. By way of example, one web site—aolsucks.org—depicts the strangulation of a cartoon figure whose head bears a striking resemblance to the AOL logo and its familiar triangular design. Surrounding the image is a collection of caustic anecdotes about the company and particularly about the quality and reliability of its services.[52] AOL might argue that its distinctive insignia, which it promotes at an annual cost in the millions,[53] is diluted when positioned beside an array of denigrating comments.

Trademark dilution is actionable under 15 U.S.C. § 1127, which defines it as the "lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence" of competition among the parties or any likelihood of confusion. Dilution can manifest itself in two ways: through "blurring," when a mark is attributed to goods or services neither produced nor delivered by the trademark owner, or through "tarnishment," when a mark is enlisted so as to taint or debase it.[54]

Dilution claims, unlike those for trademark infringement, can succeed without first establishing any likelihood of confusion. Instead, plaintiffs need only show that the mark is famous and that the defendant is blurring its distinctiveness or tarnishing its prominence through some commercial application.[55] Since this standard obviously differs from that for libel, a dilution claim, depending, of course, on the facts, may present itself as an alternative means of proceeding against a libel-proof plaintiff.

TO SUE OR NOT TO SUE

So much for theory. The question is no longer how to sue, but whether to do so at all. If the answer is yes, corporate plaintiffs should recognize the inevitable extralegal consequences and understand how to neutralize them. And, if the answer is no, the savvy lawyer will be attuned to and pre-

---

50. Thad A. Davis, *A New Model of Securities Law Enforcement*, 32 CUMB. L. REV. 69, 85 (2001-02).

51. Picker Int'l v. Leavitt, 865 F.Supp. 951, 964 (D. Mass 1994) (noting that Section 623A of the Restatement (Second) of Torts defines "commercial disparagement" as a false statement intended to bring into question quality of rival's goods or services in order to inflict pecuniary harm).

52. *See AOL Watch—Updated Daily!* available at www.aolsucks.org/aolwatch27b.htm (visited May 27, 2002).

53. *See, e.g.*, Beth Healy, *Former Thomson Financial Chief Resurfaces at Web Firm*, BOSTON GLOBE, May 21, 2000, at C5.

54. *See generally* I.P. Lund Trading ApS & Kroin Inc. v. Kohler Co., 163 F.3d 27 (1st Cir. 1998); Intermatic Inc. v. Toeppen, 947 F.Supp. 1227 (N.D. Ill. 1996); Hasbro Inc. v. Internet Entertainment Group Ltd., 40 U.S.P.Q.2d 1479 (W.D. Wash. 1996); Toys 'R' Us v. Akkaoui, 1996 U.S.Dist. LEXIS 17090 (N.D. Cal.).

55. *See, e.g.*, Ian C. Ballon, *Litigation Trends in Internet Disputes*, 691 PLI/Pat. 245, 294-96 (2002).

pared to implement any number of alternatives to litigation.

A. The Pros

The advantages to combating corporate cybersmear through litigation are two-fold. On one hand, there are upsides that exist on a purely legal plane. At the same time, formal proceedings can occasion a range of positive, extralegal effects. They can, for example, sponsor larger, systemic values and, not least of all, act as a visible and powerful deterrent for aspiring libelists.

As an altogether legal matter, successful online defamation claims serve at least two ends. First, they promote finality. By seeking appropriately broad injunctive relief, plaintiffs can rest somewhat easier knowing that if detractors succumb during litigation but later resurface, emboldened anew, they will already have an equitable judgment in hand. Unburdened by any threshold inquiries into liability, aggrieved corporations can focus on enforcement alone, and thus bring a more rapid end to their problems.

Second, a victory on the merits can establish valuable precedent. Because Internet libel is in its formative stages, visible companies subject to public scrutiny might be wise to shape the doctrines developing around cyberlibel in ways consonant with their best interests. Otherwise, lobbies on the opposite side of the aisle—the American Civil Liberties Union, the Digital Freedom Network and the Electronic Privacy Information Center, to name but a few—may make a point of getting in on the ground floor. By undertaking the defense in the early waves of cases, they may set the sort of speech-protective precedent that elevates personal freedoms over the right to seek redress of reputational wrongs in a court of law.

Extralegally, corporations emerging victorious from cyberlibel suits can generate disincentives for armchair malingers who harbor disparaging thoughts, but have yet to graft them onto some Internet outpost for mass consumption. While any publicity surrounding online defamation cases may generate bad press for the plaintiff companies, the limelight also can illuminate a blunt message: Proceed at your own risk. Because the anonymity of the Internet widens comfort zones even for the ordinarily risk-averse, it may be incumbent on corporate America to remind the public that torts are no less actionable when committed on the Internet.

From a broader perspective, cybersmear has palpable systemic effects that threaten the very evolution of the Internet. While it serves as a vehicle for entertainment and other varieties of lighter fare, the Internet is first and foremost a mechanism for gathering and disseminating information. In this sense, it was dubbed the "Information Superhighway" because of its unique potential for delivering knowledge to populations everywhere. Since information and power go hand in hand, if the Internet is impaired in its ability to share the former with the world at large, its role as the great equalizing force of the new millennium will be compromised.

Inasmuch as its essence borrows from that of a program of misinformation, cybersmear hampers public discourse that is truthful, ingenuous and thus meaningful. Veiled in anonymity and emancipated from editorial oversight, anyone with access to the Internet can spread deceptive propaganda around the globe. This might have the over-all effect of spawning vast bodies of conflicting information, the reliability of which often cannot be assessed. In this way, the Internet may be infected with falsehoods that will never be identified as such in the online marketplace of ideas.

Companies that take cyberlibelists to task will work toward eliminating this dynamic, and will thus do their part, however small, to contribute to the public good.

B. The Cons

Taking to the courts in pursuit of digital mudslingers is not without its fair share of distinct disadvantages. The biggest concern is that a lawsuit will simply exacerbate the visibility and thus the impact of the alleged defamation.

In particular, so-called "backlash" websites can be nightmares; recall the plight of Varian Medical Systems. Although the company won a series of legal victories, it thereby aroused the wrath of two past employees whom it had accused of libel. In time, making matters even worse, the backlash website gave rise to several collateral complications: republishing and a new phenomenon sometimes known as "spamdexing."

As its name suggests, republishing refers to the distribution of libelous statements through an outlet other than the original host. Such secondary outlets are usually members of the media. Spamdexing, a nouveau term of art, pertains to "a modern variant on long-utilized systems of keyword indexing."[56] Specifically, the process involves the abuse of "meta tags"—words and phrases transparently implanted in web pages to facilitate their indexing by search engines.[57]

Apparently through the manipulation of meta tags, the Varian defendants were able to raise the profile of their website on popular search engines Yahoo! and Google. Of the more than 10,800 destinations containing the phrase "Varian Medical Systems," the site operated by the defendants was listed third, directly beneath an official Varian home page.[58]

Because spamdexing can be so effective, the reach of backlash sites should not be underestimated: If properly coded, they will not necessarily wallow in obscurity.

A parade of other drawbacks can follow the decision to file suit, the cost and uncertainty of litigation marching at the head of the pack. Corporate executives should be sure to put fiscal realities before their own pride. To be attacked is not necessarily to suffer any genuine harm. Put another way, ego has no place in the process of deciding whether libelous statements threaten the sort of damages which would warrant the time and expense of litigation.

Each of the following, however, are among the many other factors properly put into the balance when exploring the expedience of initiating legal action: the potential impact on public image, especially the perception of the plaintiff as a monied corporate tyrant; the consequent costs of remedial public relations initiatives; and, finally, the difficulties in identifying and later satisfying a cash judgment against an individual defendant who is swathed in anonymity but not in wealth.

C. Alternatives to Litigation

It should come as no surprise that businesses affected by cybersmear can vindicate their rights through means other than litigation. The most common and often the simplest and most effective approach is a cease-and-desist letter. Because the Internet is a virtual costume ball—with the identities of its millions of guests hidden behind masks of an intangible sort—the perceived anonymity of online speech lulls many into a false sense of invincibility. When the mythology of unassailability is shattered on receipt of a sternly worded letter from an attorney, the average muckraker is quick to apologize and retract the causidical statements.

Taking coordinated, cooperative action with the appropriate ISP is a second possibility. Ordinarily, web surfers are required, even if only impliedly, to consent to certain terms of use before logging onto the Internet or viewing a home page.[59] The Microsoft Network, for instance,

> reserves the right at all times to disclose any information as Microsoft deems necessary to satisfy any applicable law, regulation, legal process or governmental request, or to edit, refuse to post or to remove any information

---

56. Ira S. Nathanson, *Internet Inflogut and Invisible Ink: Spamdexing Search Engines with Meta Tags*, 12 HARV. J.L. & TECH. 43, 47 (1998).

57. *See, e.g.*, DON SELLERS, GETTING HITS: THE DEFINITIVE GUIDE TO PROMOTING YOUR WEB SITE 22 (1997).

58. Search results for Varian Medical Systems, at http://google.yahoo.com/bin/query?p=Varian+Medical+Systems&hc=1&hs=1 (visited June 2, 2002).

59. Yahoo! is a perfect example. Its terms of service emphasize, "Yahoo provides its service to you, *subject* to the following Terms of Service . . . which may be updated by us from time to time *without notice* to you." Available at_http://docs.yahoo.com/info/terms (visited June 3, 2002) (emphasis added).

> or materials, in whole or in part, *in Microsoft's sole discretion.*[60]

The effect of such language is to imbue service providers with the unilateral authority to regulate their domains as they see fit. And, while the typical ISP is immunized against liability for the statements of its users, no one likes trouble. From this perspective, a corporation portrayed in a patently offensive light may discover that the ISP, which hosts the objectionable content or user, prefers to delete the material summarily or revoke the membership of the offender, rather than risk entanglement in litigation.[61]

Another option, albeit a riskier one, is to counteract cyberlibelists with a dose of their own medicine. By publicly responding to them in their own forum, a defamed company can try to set the record straight. Defusing and discrediting revilers on their own turf has the added advantage of communicating with the same general audience to which the tortfeasor first appealed. The downside, however, is that the calumniators may be provoked into intensifying their crusades. Should this occur, company officials are left with two choices, both unenviable: continue the dialogue, which could rapidly degenerate into an obtuse slugfest; or, withdraw from the exchange, which can smack of giving up or, even worse, of conceding the truth of the objectionable statements.

Last, a company may do nothing as an external matter, while at the same time taking internal steps to lay the foundation for litigation. To this end, it must preserve some evidence of the offending statements. Given the temporary nature of Internet content, the aspersive language inherently will lack permanence, and it should be documented to prepare for future legal action.

D. Corporate Pre-emptive Measures

Although it may be impossible to eliminate them entirely, both the incidence and the impact of cybersmear can be lessened by taking certain precautions. First consider the story of one Jeremy Dorosin, who had bought an espresso machine from coffee giant Starbucks. Apparently, the machine was defective, and Starbucks never sent Dorosin the complimentary coffee that was to accompany his purchase. When Starbucks refused his demand that it replace the broken machine with one costing thousands of dollars more, Dorosin took out a full-page spread in the *Wall Street Journal*. The advertisement invited readers to voice their complaints about Starbucks by calling a toll-free number that Dorosin had established, or by visiting "starbucked.com," a website that also included a detailed account of his problems with the coffee company.[62]

The advice to glean from the foregoing episode should be obvious. Preemptively register unflattering domain names that co-opt your corporate identity. Purchase Internet addresses in bulk; they can be had on the cheap. Especially for large, publicly held companies, the annual cost will be de minimis.

Next consider that the unseen enemy is bad enough, but that the unknown enemy is even worse. Accordingly, businesses must devise some means of monitoring the Internet for defamatory materials concerning them, their products and services, as well as their individual officers, directors and key employees. All but the largest entities will be best served by outsourcing this responsibility to any of the growing number of third-party services that specialize in scouring the web for derogatory references to their corporate clients.[63]

---

60. Available at http://privacy.msn.com/tou (last modified March 2002) (emphasis added). Weighing in at a total of nearly 9,000 words, the MSN terms of use span some 25, single-spaced pages.

61. *See, e.g.*, Ronald F. Lopez, *Corporate Strategies for Addressing Internet "Complaint" Sites*, 14 INT'L L. PRACTICUM 101, 104 (2001).

62. *Id*.

63. eWatch L.L.C. is perhaps the leading such service. Information about it is available at http://ewatch.com/about_ewatch.html (visited June 3, 2002) (describing a range of corporate intelligence solutions). Another prominent member of this burgeoning "cottage industry" is Connecticut-based CyberAlert Inc. *See* Shaun B. Spencer, *CyberSLAPP Suits and John Doe Subpoenas*, 19 J. MARSHALL J. COMPUTER & INFO. L. 493, 494 n.9 (2001).

Third, the prudent company will plan now for what has yet to come. Vicious rumors can materialize on the Internet out of nowhere, and will sometimes spread like wildfire. If it becomes necessary to undertake some form of damage control, a contingency plan—or the lack thereof—may mean the difference between the effective and the feckless response strategy. Caught off guard, a firm layered in bureaucracy may struggle to first formulate and then execute a rapid, but still measured rejoinder.

Last, a timeless truth deserves repeating. Those closest to us sometimes hurt us most. For present purposes, the sentiment is intended to underscore the fact that corporate cyberlibel recurrently comes from within.[64] Although employers can exercise little or no control over the after-hours activities of their employees, vigilant companies can regulate behavior to a much greater extent during the work day. Woefully behind the times is any modern business that has yet to promulgate and enforce stringent company policies for the use of electronic mail and of the Internet generally.

While some employees will inevitably break the rules, others at least will reflect on them and think twice before using an office computer to speak out against their employer. With such policies in place, transgressive employees also may subject themselves unwittingly to liability not only in tort, but also in contract.

CONCLUSION

To call the Internet a new frontier is by now a misnomer. Its reach is global, its content consumed by billions, and almost anyone with a computer can tap its power. The Internet is becoming a bully pulpit from which the disgruntled broadcast their frustrations to the world at large.

Squarely in their crosshairs—much like politicians, celebrities and other magnets for public attention—will be corporations the world over. Because that much is inevitable, companies today must understand the intricate contours of the problem, appreciate both their legal and extralegal options, and prepare themselves—now, rather than later- for the trouble that will eventually come knocking.

---

64. *See, e.g.*, Matthew S. Effland, *Digital Age Defamation*, 75 FLA. B.J. 63, 63-64 (2001) (observing that damaging comments made by disgruntled employees about company business practices is not new phenomena, but suggesting that Internet has magnified problem); Daniel P. Schafer (Note), *Canada's Approach to Jurisdiction over Cybertorts*, 23 FORDHAM INT'L L.J. 1209-10 (2000) ("Since [Internet] bulletin boards provide an easy and inexpensive way for a speaker to reach a large audience, disgruntled . . . employees have used them to voice their concerns over a company, regardless if the complaints are justified.") (footnote omitted).

The Privacy Project

Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace

Employers should have detailed, understandable and fair computer, e-mail and Internet usage policies impartially administered

The evil that men do lives after them;
The good is oft interred with their bones;
—William Shakespeare, Julius Caesar, Act III, scene 2

I have come to believe that if anything will bring about the downfall of a company, or maybe even a country, it is blind copies of e-mails that should never have been sent in the first place.
—Michael Eisner (commenting to the graduating class at the University of Southern California)

I suggested deleting some language that might suggest we have concluded the release is misleading.
—E-mail sent by Nancy Temple, in-house counsel for Arthur Andersen, referring to an e-mail that was central to the jury's decision to convict the accounting firm

By William G. Porter II and Michael C. Griffaton

WITH JUST a few clicks of a mouse, an employer may lose valuable trade secrets and confidential information, be liable for violating copyright laws, or be exposed to claims that it permitted a hostile work environment. The pervasive and ubiquitous nature and exponential growth of electronic mail and the Internet highlight the need to monitor the electronic workplace to curb that liability.

Just consider:

- The number of e-mail users increased from 8 million in 1991 to 108 million in 2000.[1] In 2000, 40 million employees exchanged more than 60 billion messages daily.[2]
- According to a 1999 study by the American Management Association, at least 50 percent of all workplace Internet activity is not business-related.[3]
- A study by the ePolicy Institute found that 85 percent of employees admit to recreational surfing at work.[4] Seventy percent of employees admitted to receiving or sending adult-oriented personal e-mails at work, while 60 percent admitted to exchanging e-mail that could be considered racist, sexist or otherwise "politically in-

IADC member William G. Porter II is a senior partner at Vorys, Sater, Seymour and Pease LLP in its Columbus, Ohio, office, where he concentrates his trial practice in business and employment disputes. He is a graduate of Amherst College (1978) and Case Western Reserve University School of Law (1984).

Michael C. Griffaton is an associate in the same firm and concentrates in employment law. He is a graduate of Ohio Wesleyan University (1990) and Case Western Reserve University School of Law (1993).

1. Edward Morawski, *The Internet Around the World: Rising to the Challenge* (Spring 2001) (online at http://www.angusreid.com/pdf/publicat/fow_art.pdf).
2. Jay P. Kesan, *Cyber-Working or Cyber-Shirking: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 289 (2002).
3. Samuel Greengard, *The High Cost of Cyberslacking*, 79 PERSONNEL J. 2224 (December 1, 2000).
4. Elron Software, *1999 Email Abuse Study* (online at www.elronsw.com/pdf/1999_Email_Study.pdf). *See also 2001 Electronic Policies and Practices Survey*, available at www.epolicyinstitute.com/survey/index.html

correct." Most traffic to Internet pornographic sites occurs during regular business hours, probably because Internet connections usually are faster in the workplace.

Companies have taken note of these statistics and have adopted e-mail and Internet usage policies that may contain provisions for continuous or random monitoring of usage. The ePolicy Institute study reports that 77 percent of employers monitor employees' e-mail and Internet use. In fact, 10 percent of workers with e-mail/Internet access (about 14 million people) are under continuous online surveillance.[5] About two thirds of employers have disciplined or terminated employees for violating electronic usage policies.[6]

Employers give several reasons for monitoring. Generally, they wish to maintain their professional reputation and image. They also are concerned with employee productivity and business efficiency, as "cyberslacking accounts for 30 to 40 percent of lost worker productivity."[7] With respect to legal liability, one commentator has stated, "Via the recent expansion of the strict liability doctrine of respondeat superior, an employee may be held strictly liable for the foreseeable torts and crimes of employees."[8] Therefore, monitoring may assist employers in preventing and discouraging sexual or other illegal workplace harassment, defamation, copyright violations from the illegal downloading of software, music and movies, and the deliberate or inadvertent disclosure of trade secrets and other confidential information. The ePolicy Institute study showed that 68 percent of employers that monitor cite legal liability as their primary reason.

No federal or state statute currently prohibits employers from monitoring their electronic workplace. The federal Electronic Communications Privacy Act and similar state laws provide some limitations, but these limitations can be overcome in the workplace through various exceptions in the statutes.[9] The federal act prohibits the interception of electronic communications such as e-mail. It defines "interception" to mean the "contemporaneous acquisition of the communication," so an interception takes place only when an individual sends an e-mail and a third party is able to obtain a copy of the transmission at the time it is sent.

In reality, however, the act provides employees little protection from the monitoring of their workplace electronic communications. It does not apply to e-mails in their "stored" state. This means that employers can freely obtain copies of e-mails from a network computer or the employee's hard drive without violating the act. Even when the employer intercepts electronic communications, monitoring is permitted when done in the "ordinary course of business" or when the employee has "consented" to it.

Moreover, few states (among them, Delaware and Connecticut) even require that employers notify their employees of monitoring.[10]

As a general matter, employees in the private sector have no reasonable expecta-

---

5. *14 Million U.S. Workers under Continuous Online Surveillance*, July 9, 2001 (online at www.privacyfoundation.org/resources/14million.asp).

6. Greengard, *supra* note 3.

7. Russell J. McEwan & David Fish, *Privacy in the Workplace*, 23 N.J. LAW. 20 (February 2002), *citing Workers Surf at Your Own Risk*, Business week.com, June 12, 2000.

8. Kesan, *supra* note 2, at 311, *citing* John Edward Davidson, *Reconciling the Tension Between Employer Liability and Employee Privacy*, 8 GEO. MASON U. CIV. RTS. L.J. 145, 147 (1997).

9. 18 U.S.C. § 2510 (2002). For an overview of the Electronic Communications Privacy Act, *see* Kesan, *supra* note 2, at 295-301. *See also* N.J. STAT. ANN. 2A:156A-1 *et seq*. (2002); N.Y. PENAL LAW 250.00 *et seq*. (2002); 18 PA. CONS. STAT. ANN. 5701 *et seq*. (2002).

10. *See* DEL. CODE ANN. tit. 19, § 705 (2002) ("No employer . . . shall monitor or otherwise intercept any . . . electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer either: (1) provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer provided E-mail or Internet access services; or (2) has first given a one-time notice to the employee of such monitoring or intercepting activity or policies.") *See also* CONN. GEN. STAT. § 31-48d (2002) ("each employer who engages in any type of elec-

tion of privacy in their workplace e-mail and Internet usage that otherwise would abrogate the employer's right to monitor that usage. In fact, courts almost expect that employers will engage in some form of monitoring. As the Seventh Circuit explained in *Muick v. Glenayre Electronics*:

> The laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as medium of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that failure to do so might well be thought irresponsible.[11]

E-mail and Internet privacy issues were addressed in the *Defense Counsel Journal* in 2000 by Hall Adams III, Suzanne M. Scheuing and Stacey A. Feeley in *E-Mail Monitoring in the Workplace: The Good, the Bad and the Ugly*.[12] Their paper addressed the central issue of whether an employer can legally monitor employee e-mails and Internet usage without violating employees' privacy or some other state or federal law. The answer to that question was essentially, yes; the courts have consistently rejected claims that e-mail and Internet monitoring represents and invasion of privacy.

This article surveys the flip side of the employer's right to monitor: an employer's liability for actually acquiring information through electronic monitoring, having that information and potentially acting—or failing to act—on that information. In many respects, this delves into uncharted areas of cyberlaw, as the courts are just beginning to explore what liability, if any, employers may have in this arena.

E-MAIL AND INTERNET USE: EMPLOYEES' CONDUCT AT WORK

Employers have always monitored workplace conduct. In *O'Connor v. Ortega*,[13] for example, the U.S. Supreme Court recognized that employers have legitimate interests in monitoring their employees' work environment.

A. Sexually Explicit E-mails

In the Seventh Circuit *Muick* case, cited above, federal law enforcement authorities notified Glenayre Electronics, Albert Muick's employer, that they were investigating Muick's dealings with child pornography. At their request, Glenayre seized Muick's workplace computer until the authorities obtained a warrant for it. Muick claimed that Glenayre's actions constituted an unreasonable search and seizure and a violation of his right to privacy.

The court first rejected Muick's claims that the company conducted an illegal search or violated his constitutional rights by cooperating with federal investigators because Glenayre was not acting as a government agent when it turned over the computer to the authorities. Next, the court rejected Muick's right to privacy claim to the computer the employer had furnished for use in the workplace, noting that "Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim." The case reinforces the importance of a properly drafted e-mail policy to prevent employees from succeeding in an invasion of privacy claim.

In *Blakey v. Continental Airlines*,[14] Tammy Blakey, Continental Airlines' first

---

tronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur. Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice." An employer may conduct monitoring without prior written notice when it has reasonable grounds to believe that employees are engaged in conduct which violates the law, violates the legal rights of the employer or the employer's employees, or creates a hostile workplace environment, and electronic monitoring may produce evidence of this misconduct.).

11. 280 F.3d 741, 743 (7th Cir. 2002) (parenthetical by the court).
12. 67 DEF. COUNS. J. 32 (2000).
13. 480 U.S. 709, 722 (1987).
14. 751 A.2d 538 (N.J. 2000).

female pilot on the A300 Airbus aircraft, sued Continental in federal court for sexual harassment, discrimination and defamation. During that litigation, a number of Continental pilots posted insulting, defamatory and derogatory remarks about her on the pilot's online computer bulletin board, which was accessible via the Internet by all Continental pilots and crew members through their paid membership in CompuServe. Blakey sued Continental and several coworkers who posted messages on the bulletin board in state court for, among other things, retaliatory sexual harassment.

The New Jersey Supreme Court explained that an employer can be held liable for co-workers' retaliatory harassment if it knew, or should have known, about the harassment but failed to act to stop it, and employers have a duty to take effective measures to stop that harassment in the workplace and settings related to the workplace. Consequently, Continental's liability would depend on whether the on-line forum was such an integral part of the workplace that harassment there should be regarded as a continuation or extension of the pattern of workplace harassment. The case was remanded to the trial court for that determination.

It is notable that the Blakey court did not hold that employers have a duty to monitor private communications of their employees, but it did admonish employers that "it may well be in [their] best interests to adopt a proactive stance when it comes to dealing with co-employee harassment," adding that "the best defense may be a good offense." Effective remedial steps reflecting a lack of tolerance for harassment will be relevant to an employer's affirmative defense that its actions absolve it from all liability for sexual harassment. This case was unusual because the employer did not own the computer network at issue. Where the employer does so, as in most cases, it will be nearly impossible to argue that what occurs on the employer's own computer network is not an extension of the workplace.

In *Strauss v. Microsoft Corp.*,[15] Karen Strauss, a female employee, sued Microsoft for gender discrimination in failing to promote her, relying in part on sexually related e-mails she received from her supervisor as evidence of gender bias. The e-mails included an advertisement for "mouse balls," a news report on Finland's proposal to institute a "sex holiday," a parody of a play entitled "A Girl's Guide to Condoms," and a message entitled "Alice in Unix Land" that mixed computer language with sexual references. Some of the e-mails were not sent directly to Strauss but by the supervisor to another employee, who, in turn, forwarded them to the rest of the staff.

The U.S. District Court for the Southern District of New York denied Microsoft's motion for summary judgment, concluding that a jury could find pretext for gender discrimination based on the e-mails. Monitoring e-mail could have revealed this conduct and possibly short-circuited the "harassment" of which Strauss complained.

Finally, in *Coniglio v. City of Berwyn*,[16] Susan Coniglio was employed by the City of Berwyn as manager of the its computer department. Allen Zank, the city comptroller, was her direct supervisor. Coniglio alleged that, among other things, Zank regularly viewed pornography on the Internet, in full view of her and other city employees, would print out pornographic pictures and store them in binders in his office, and would invite her into his office and attempt to elicit her reaction to sexually explicit pictures on his computer screen. She testified that the women were sometimes pictured in different sexual positions with creatures resembling medieval gargoyles. Coniglio complained of Zank's behavior, and Zank later terminated her.

She sued, alleging in part that Zank's behavior created a hostile work environment. The U.S. District Court for the Northern District of Illinois denied the city's motion for summary judgment on this claim.

Both *Strauss* and *Coniglio* highlight the importance of e-mail and sexual harass-

15. 814 F.Supp. 1186 (S.D. N.Y. 1993); *see also* 1995 WL 326492 (S.D. N.Y.).
16. 2000 WL 967989 (N.D. Ill.).

ment policies. Just as calendar "pin-ups" are no longer acceptable in the workplace, on-screen pornographic or sexual images are not acceptable and can be evidence of a hostile work environment. While the employers in those two cases ultimately may prevail at trial, defense of the cases (like most litigation) will be costly in terms of money, time and negative publicity.

While most employees have been trained about improper office behavior—for example, sexual harassment—many do not view e-mail as an avenue for harassment and tend to treat their incoming and outgoing messages more casually than a letter or memo written on company letterhead. In one case that garnered considerable press coverage, Chevron paid female employees $2.2 million in 1995 to settle a sexual harassment lawsuit from inappropriate e-mail, including "25 Reasons Why Beer is Better than Women," sent by male employees, including male supervisors.[17]

In *Faragher v. City of Boca Raton* and *Burlington Industries Inc. v. Ellerth*,[18] the U.S. Supreme Court made employers liable for the wrongful action of supervisors that result in adverse employment action, even if the employers were unaware of specific actions involved or taken. If employers fail to take affirmative steps to prevent sexual harassment, they are exposing themselves to potentially larger damage awards. Of course, it is likely that the more an employer monitors its e-mail and Internet usage, the more responsibility the employer will be assessed for its content. As the New Jersey Supreme Court pointed out in *Blakey*, the best defense may be a good offense, and monitoring e-mail and Internet usage may be that "good offense."

B. Trade Secrets and Confidential and Proprietary Information

The National Counterintelligence Agency estimates that businesses lost $44 billion due to economic espionage in one 17-month period.[19] Employers' greatest risk to their computer security comes not from outside hackers but from current and former employees who deliberately or inadvertently disclose confidential or sensitive information. According to a 2001 survey by Elron Software, more than 40 percent of respondents admitted to receiving company confidential information such as client lists, financial statements and product specifications from "outside their organizations—a 356 percent increase since 1999."[20] Employees no longer have to photocopy documents surreptitiously; they can simply download reams of data to disk, CD or DVD, or even e-mail the information to a competitor with the click of a mouse.

For example, a former executive of Borland International, a software company, was accused of e-mailing trade secrets to a competitor, which happened to be his new employer, before he quit Borland. Criminal charges were filed, but eventually dropped, and the civil dispute was quietly settled.[21]

In *Frasier v. Nationwide Insurance*,[22] Nationwide searched its file server and located e-mail communications that revealed its employee, Richard Frasier, had e-mailed correspondence critical of Nationwide's business practices to a competitor. Soon after discovering this, Nationwide terminated Frasier. Frasier sued, alleging that Nationwide had unlawfully intercepted his e-mail communication in violation of

---

17. Liz Stevens, *Today's Technology Makes It Easier for Supervisors to Watch Workers*, MILWAUKEE J. SENTINEL, October 6, 1999, at 3.

18. 524 U.S. 775 (1998) and 524 U.S. 742 (1998).

19. James E. Hudson III, *Trade Secret Theft Threatens Everyone with Corporate Economic Espionage Escapades*, HOUSTON BUS. J. TECH. Q., October 1, 1999 (online at http://www.bizjournals.com/houston/stories/1999/10/04/focus13.html).

20. Elron Software, *The Year 2001 Corporate Web and Email Study*, 5 (2001) (online at http://www.elronsoftware.com/pdf/NFOreport.pdf).

21. *See* Garry G. Mathiason & Roland M. Juarez, *The Electronic Workplace: An Overview*, CEB CALIF. BUS. L. R. 188, 189 (1995). *See* California v. Eubanks, 927 P.2d 310 (Cal. 1996), *as modified and rehearing denied*, 1997 Cal. Lexis 1016 (software company paid for services of two computers experts to assist prosecutor).

22. 135 F.Supp.2d 623 (E.D. Pa. 2001).

state and federal wiretap laws and had unlawfully accessed his e-mail from storage in violation of stored communication laws.

The federal district court for the Eastern District of Pennsylvania rejected both contentions, first, because there was no "interception," and, second, because the employer had lawfully accessed its own equipment and "stored" e-mail to obtain the information.

An electronic monitoring policy may help the employer uncover such activities, perhaps in time to prevent what could be substantial damage to the employer's business.

C. Copyright Infringement

Employers also may be needlessly exposed to lawsuits for copyright violations if they permit (or ignore the fact that) employees to receive and/or download software or other materials, such as music, video and graphics files, from e-mail systems or the Internet. Copyright infringement can result in civil and criminal penalties, not to mention adverse publicity. Electronic monitoring is an effective way to minimize that legal exposure for copyright infringement.

Northwestern University, for example, fired Carla Tomina, a secretary who had amassed more than 2,000 MP3 music files on her work computer. While Tomina claimed the files came from her own CD collection, as opposed to those on a website like Napster, the university had been contacted by at least one music copyright holder in connection with unauthorized, downloaded works.[23]

Another company agreed to a $1 million out-of-court settlement with the Recording Industry of America because the company had maintained a computer server that employees used specifically for downloading, storing and sharing MP3 files.[24]

E-MAIL AND INTERNET USE BEYOND THE WORKPLACE

Most electronic monitoring by employers, like the monitoring of employees' conduct in general, is conducted in the workplace, but employers also monitor and even discipline employees' off-duty conduct. A common example of monitoring is investigating whether workers' compensation claimants are in fact working when they claim to be unable to do so. An example of discipline is terminating of an employee who comes to work under the influence of drugs or alcohol. Electronic monitoring expands the employer's potential range of surveillance and the potential liability for invasion of privacy.

Generally, employees are unsuccessful in claims if the employer can establish a nexus (however somewhat tangential) between the off-duty conduct and the workplace. Some states, such as New York, have made it unlawful to discriminate against employees based on their "legal recreational activities outside work hours, off the employer's premises and without use of the employer's equipment or property." "Recreational activities" means "any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies or similar material."[25] Statutes such as this one may limit an employer's ability to discipline employees for their off-duty, personal e-mail and Internet use.

Many people operate their own websites for personal interests ranging from genealogy to pornography. George and Tracy Miller, for example, were fired from their nursing positions at an Arizona hospital for operating an Internet pornography site showing the Millers engaged in sexual intercourse. They claimed was they operated the site to make money for their children's

---

23. Casey Newton, *Downloading MP3's Gets NU Employee Downsized*, THE SUMMER NORTHWESTERN, July 26, 2001 (online at http://www.polarity1.com/pcrr3.html).

24. Benny Evangalista, *Deleting Download: Companies Concerned over Employees' File-Sharing at Work*, S.F. CHRON., June 3, 2002 (online at http://www.websense.com/company/news/companynews/02/060302.cfm).

25. N.Y. LAB. LAW 201-d.

college education. Hospital computer staff alerted hospital administrators that employees were logging onto the site while at work. The hospital initially suspended the Millers pending investigation, and then terminated them, stating that their website created a hostile environment for the hospital's employees. The hospital noted that the Millers had signed a policy statement that provided employees could be discharged for "immoral or indecent conduct" while on or off duty.

The Millers initially filed a charge of discrimination with the Equal Employment Opportunity Commission and received a right-to-sue letter. (It's unclear the protected class into which the Millers would fall.) However, they elected not to pursue the claim and, instead, are now radio talk show hosts.[26]

According to an article in the *Sun-Herald* in North Port, Florida, in March 2001, police officer Daniel Lake was suspended for three days for "conduct unbecoming an officer" for pornography-related activities. The officer, who had a record described as "excellent," was not personally involved with the pornography. Rather, his wife had submitted pornographic images of herself to a voyeuristic website as a birthday present for her husband. While some residents reportedly were opposed to the suspension, police officials were adamant in their belief that they had the right to regulate the personal conduct of a police officer's family.[27]

Bill Owens, a Maryland Home Depot salesman, claimed that his supervisors ignored blatant sexual harassment by a female coworker because he and his wife operated a live sex video streaming site. In May 1999, a female coworker called him "Buck Hunter," his web site pseudonym, asked him for oral sex, exposed her breasts to him and grabbed his crotch in full view of customers. Owens quit because he was afraid of having his secret identity revealed. When he later went back to his supervisor to try to work things out, the supervisor was helpful "until he heard about the site." Owens alleged that his supervisor said that he can protect him from being grabbed but can't do anything about what people say. Of course, the supervisor is legally incorrect, but Owens ultimately decided not to sue.[28]

Finally, in October 2001, a Georgia police officer sent an e-mail to an online discussion list that advocated "eliminating the entire Arab world" if terrorism continued and suggested that that United States bomb Mecca so that Muslims would be forced to pray "at a crater 25 miles across." The officer had created the discussion list as a forum for law enforcement officers, and the list was not officially tied to any law enforcement agency. The officer's e-mail message, however, carried his professional e-mail signature, which identified him as a police officer. Subscribers to the list complained to the police chief, and the officer agreed to resign.[29]

PROTECTION UNDER NATIONAL LABOR REALTIONS ACT

A. Introduction

Employer monitoring of e-mail and Internet usage raises a host of labor law issues. Under Section 8(a)(1) of the National Labor Relations Act (NLRA), employers are prohibited from giving even the impression of surveillance of employees' union activity. As the National Labor Relations Board (NLRB) explained, "Employees should be free to participate in union organizing campaigns without the fear that members of management are peering over their shoulders, taking note of who is in-

---

26. After Hours, abcNEWS.com, December 9, 1999 (online at abcnews.go.com/onair/2020/transcripts/2020_991209_onlineporn_trans.html); *Cyber porn Nurse: "I Feel Like Larry Flynt"* (online at http://zdnet.com.com/2100-11-515178.html?legacy=zdnn).

27. Elaine Allen-Emrich, *Residents React to Recent City Internet Sex Scandal* (online at http://www.sun-herald.com/search/search.asp?showarticle=117710).

28. John Simons, *X-tracurricular Activities*, Business 2.0 (January 2001) (online at www.business2.com/articles/mag/0,1640,14445,ff.html).

29. Erin McClam, *Ga. Cop Asked to Resign for E-mail*, AP Online, October 4, 2001, reported at 2001 WL 28748621.

volved in union activities, and in what particular ways."[30] Electronic monitoring enables employers to record information about the employees and their activities, often without the employees even realizing it.

Within the past several years, the NLRB General Counsel's Office has considered several cases involving employer limitations on employee use of company e-mail and computers. The employers generally maintained "no solicitation/no distribution policies" prohibiting dissemination of non-business-related messages through internal e-mail systems. The lead case in this area is *Pratt & Whitney*,[31] in which the general counsel challenged the legality of a business-only e-mail policy. At issue was the use of e-mail by the company's 2,450 professional and technical employees who worked in one department and communicated extensively via e-mail. The general counsel reasoned that Pratt & Whitney's policy prohibiting all non-business use of a company's e-mail and computer system was overbroad and facially unlawful.

Pratt & Whitney's written policy prohibited the use of computer resources for non-business, unauthorized or personal purposes However, the policy was not strictly enforced, and employees often violated it. After a union organizing campaign was underway, the employer disciplined several employees who were union activists for sending e-mail messages and downloading union-related information onto the company computer. After finding that the employer violated the NLRA by disparately and discriminatorily enforcing its policy only against employees sending union messages, the general counsel outlined a new theory, derived from no-solicitation and no-distribution case law, that the mere existence of a business-only policy violates the NLRA—in effect, that a business-only policy was similar to a no-solicitation policy.

In labor law parlance, no-solicitation rules prohibit employees from communicating to fellow employees for various causes, including union organizing. To be lawful, a no-solicitation rule must be non-discriminatory (it cannot apply just to union organizing), and it must apply only to solicitations that take place in work areas during working time. A company may not ban solicitation by employees during non-working time, whether or not it occurs in a work area. No-distribution rules prohibit the distribution of literature on the employer's premises, and they also must be non-discriminatory. However, a company may lawfully ban distribution of materials in work areas at any time, whether working or non-working, but in most industries, an employer cannot ban distribution by employees in non-work areas.

In the *Pratt & Whitney* opinion, the general counsel first concluded that employee computer workstations were work areas. Next, the opinion noted that the employer's e-mail system was used as a tool for conversations and that the business-only rule prevented the employees from conversing about the union during their non-working time. Accordingly, this is as unlawful as a no-solicitation rule that bans solicitation during non-working time.

B. Recent Cases

In an NLRB general counsel case, *TXU Electric*,[32] the employer adopted this e-mail policy:

> Internet, Intranet and E-mail are provided by the Company for business-related use. Any personal use by Users must be kept to a minimum (no more than five (5) User I.D.'s per E-mail), must comply with all Company policies, and must not involve sending or storing files which consume large amounts

30. Flexsteel Indus. Inc., 311 NLRB 2547 (1993). For an overview of the union-related issues surrounding e-mail, Internet usage, and electronic monitoring in the workplace, *see* Frederick D. Rapone Jr., *This Is Not Your Grandfather's Labor Union—Or Is It? Exercising Section 7 Rights in the Cyberspace Age*, 39 DUQ. L. REV. 657 (2001); Gwynne A. Wilcox, *Section 7 Rights of Employees and Union Access to Employees: Cyberorganizing*, 16 LAB. LAW. 253 (2000).

31. 1998 WL 1112978 (NLRB General Counsel, February 23, 1999).

32. 2001 WL 1792852 (NLRB General Counsel, February 7, 2001).

> of computer storage space. Personal E-mail should not exceed one-half (1/2) page in length or contain photographs, video or file attachments. Additionally, sending chain E-mail or non-business related bulk E-mail is prohibited. Users may not use Company resources to create a personal home page, web page, or computer programs.

The union contended that the employer's e-mail unlawfully restricted employees and union representatives from the exercise of their rights under the NLRA. The general counsel disagreed, concluding that the policy was facially lawful because it permitted employees to use the e-mail system for personal use but only limited the length of the message and the number of employees to which a particular e-mail may be sent. The opinion held that the policy narrowly addressed the employer's legitimate business concerns—to forestall significant interference with its use of the e-mail system—while adequately balancing employees' Section 7 rights and the employer's managerial interests.

Such limitations are lawful, according to the general counsel, as there was sufficient evidence demonstrating a substantial business justification that unfettered personal use would impair the effectiveness of the e-mail system significantly. Because there was no restriction on the number of e-mails that employees could send (as opposed to size the e-mail messages), employees still had the opportunity to communicate effectively throughout the bargaining unit.

In *IRIS-USA*,[33] the general counsel upheld a ban on all personal e-mail where the computers were not part of the employees' work area. Because the employees did not use computer or e-mail as part of their regular work, a work area "did not exist for them."

Sitel Corp.[34] highlights the fact that employees' right to concerted activity guaranteed by the NLRA applies in both the union and non-union workplace. The e-mail policy in question restricted the use of the employer's computer and e-mail system to work-related purposes. The employees, who were not represented by a union, had regular access to a computer network, including e-mail and the Internet. An employee named Scully was disciplined after he forwarded an e-mail from a former employee regarding working conditions at Sitel. It was well-known at Sitel among both management and employees that employees commonly used the computer system, the Internet, and e-mail for numerous non-work-related purposes.

Scully won a Pyrrhic victory. The general counsel determined that the company's e-mail policy was unlawfully overbroad and that the company unlawfully disciplined Scully for criticizing the working conditions.[35] The opinion went on, however, to note that the company eventually —and lawfully—discharged Scully for viewing pornographic web sites on his computer. This case highlights the importance of monitoring employee Internet activity.

C. Observations and Unanswered Questions

The NLRB general counsel's advice memoranda raise, but do not answer, several questions about the scope of the traditional no-solicitation and no-distribution rules. Under the well-established no-distribution rule, an employer can ban distribution of materials in work areas at any time; an employer may not ban solicitation that occurs on non-work time regardless of where the solicitation occurs. If an employee does not have set break times, it is difficult to draw the line between non-work and work time. If the employee sends an e-mail to all fellow employees about working conditions and the employees read the e-

33. 2000 WL 257107 (NLRB General Counsel, February 2, 2000). *See also* Emcompass Services Corp., 2001 WL 310613 (NLRB General Counsel, January 18, 2001).

34. 2000 WL 33252020 (NLRB General Counsel, October 5, 2000).

35. *See also* Timekeeping Sys., 323 NLRB 244 (1997) (employee who sent e-mail to other employees critical of company's vacation policy was engaged in "concerted activity," which is protected by the NLRA; company president's termination of employee because employee refused to publicly apologize for sending e-mail was unlawful; employee reinstated with back pay).

mail while at their desks, is that e-mail a "solicitation" or a "distribution"? If an employee with an established break time reads the e-mail in his work area when he is not on break, does the e-mail then become a prohibited distribution and solicitation? What if the employee is on break but is in his work area, is the e-mail a distribution (material read in the work area) or a solicitation (material read on non-work time)? What happens if the employee prints out the e-mail and reads it in the break room?

There are no easy answers to those and the myriad other scenarios that may arise as e-mail use continues to proliferate. At this point, the NLRB general counsel has provided little guidance for employers.

One thing that is clear, as the above cases point out, is that an employer generally cannot discipline an employee because of the content of the employee's e-mail message. Depending on the scope of the e-mail policy, however, the employer may be able to discipline an employee because the employee violated the e-mail policy, for example, by sending pornographic images or file attachments that are too large, or by sending the e-mail to too many recipients.

NAVIGATIONAL AIDS FOR THE ELECTRONIC WORKPLACE

Once the employer begins to monitor employees' e-mail and Internet usage, what happens to all the saved e-mails and Internet history logs? How long is that information saved? How long should it be saved? What should the employer do with all the information it has logged through its electronic monitoring efforts?

A. Electronic Discovery

First and foremost, employers (and employees) must remember that e-mail is not necessarily gone when "deleted." The informality of e-mail and the mistaken belief that it can be erased easily often result in the creation of evidence that can make or break a case. Electronic evidence that can be monitored includes not just e-mail and Internet usage, but it also includes computer user files, applications, databases, spreadsheets, network log files, access activities, back-up tapes, data remnants, metadata, and deleted files. Rule 26(a) of the Federal Rules of Civil Procedure requires parties disclose computer-based evidence that they may use to support their claims or defenses, and Rule 34 has been interpreted to mean that electronic documents must be produced in their "native format."[36]

Employers also must remember that document destruction is not permitted simply because no subpoena has been served or because litigation has not commenced. Some courts do not consider destruction of potential evidence before a lawsuit is filed as spoliation, while others find that a duty to preserve documents arises when a party should reasonably know that litigation is imminent. Some courts presume that document destruction under a company policy is innocent, while others question whether a duty to preserve was triggered regardless of such a policy.

The traditional approach to reducing the legal risk with old e-mail messages is to create written policies that define the "useful life" of different document types and thereby limit the spread of information. Moreover, various state and federal administrative agencies require certain documents to be preserved for periods of time. For example, Title VII of the Civil Rights Act generally requires that any personnel or employment record be preserved for one year after the date the record was made or the undertaking of the personnel action involved, whichever is later. If an employee is involuntarily terminated, such records must be kept for one year following the date of termination.[37]

Hand-in-hand with monitored information is deciding how long to retain it. Current storage media make it easy and inexpensive to save almost everything indefinitely. Of course, this also makes it easy to "forget" that the information is there. The most telling example of docu-

36. United States v. Microsoft Corp., 1998 WL 699028 (D. D.C.).

37. 29 C.F.R. §§ 1602.14; 29 C.F.R. § 1627.3(b).

ment retention and destruction problems is the Arthur Andersen trial resulting from the Enron bankruptcy. The Andersen policy called for the retention of important company documents but the destruction of extraneous records. Andersen lawyer Nancy Temple sent an e-mail on October 12, just five days before the Securities and Exchange Commission opened an informal inquiry into Enron, reminding workers of the policy.[38] David Duncan, the former Andersen lead auditor for Enron and the government's chief witness in the case, testified during the trial that he "obstructed justice" by "instruct[ing]people on the team to follow the document retention policy, which I knew would result in the destruction of documents."[39]

Destruction of documents can be costly in more ways than one. In one case, a court fined Prudential Insurance $1 million for its "haphazard and uncoordinated approach to document retention" in face of a court order requiring retention, even though there was no proof that Prudential intended to thwart discovery. The court also instructed the jury that it could draw an adverse inference that destroyed documents were relevant and unfavorable to Prudential.[40]

Courts have upheld requests for production of documents that required companies to spend thousands, and even tens of thousands, of dollars to retrieve "deleted" information or information stored on back-up tapes and servers. In one case, the defendants were ordered to bear the cost of searching through 30 million pages of e-mail despite their estimate that it would cost between $50,000 and $70,000. It is notable that the court stated, "If a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."[41]

Litigation is costly in any event. Electronic discovery battles can be even more costly.[42]

B. Electronic Monitoring Policies

Employers considering monitoring their electronic workplace are well advised to create a monitoring policy detailing the types of monitoring used and why, explaining what kinds of e-mail or Internet usage is allowed and what is not. Included in the policy should be the actions that will be taken if the policy is violated. Employers must notify employees of the monitoring and should ensure that the employees return a signed acknowledgment of their understanding of the policy and of the ramifications for violating it.

Like other policies, the electronic monitoring policy should be re-evaluated periodically, and any revisions should be redistributed, signed and returned by the employees. Employers also should update their anti-harassment policies to include specific references to inappropriate e-mail and Internet usage. Finally, employers must train and periodically remind managers and employees of the policy.[43]

Employers can take computer monitoring a step further than merely looking through computer files; they can use the computer itself to help by employing a plethora of software designed specifically to monitor computer activity. One manufacturer of monitoring software even claims to be able to detect potential workplace violence from monitoring employees' e-mail.[44]

---

38. Jonathan Weil et al., *Andersen Win Lifts U.S. Enron Case*, WALL ST. J. June 17, 2002, at A1.

39. Milton Lawson, *Duncan Testifies about Shredding*, WASH. TIMES, May 14, 2002 (online at http://www.washtimes.com/upi-breaking/14052002-023744-292lr.htm).

40. In re Prudential Ins. Co. Sales Practices Litig., 169 F.R.D. 598, 617 (D. N.J. 1997).

41. In re Brand Name Prescription Drugs Antitrust Litig., 1995 U.S.Dist. Lexis 8281 (N.D. Ill.).

42. *See* Jason Krause, *Electronic Documents Are Vital to Building a Case, So Don't Get Papered Over*, ABA J. July 2002, at 49; Kevin L. Carr, *Electronic Data: The Legal and Practical Aspects of Retrieving Electronic Data in Discovery*, ABA Labor and Employment Law Section (Midyear Meeting, March 2001).

43. *See* Torianne Florentino, *Employee Privacy in the Ever-Evolving Workplace*, 701 PRAC. L. INST. 679, 702-704 (2002).

44. *See* John C. Dvorak, *Monitoring the Emotional State*, Forbes.com, May 5, 2001 (online at www.forbes.com/2001/05/14/0514dvorak.html (discussing Stroz Associates).

Monitoring software generally falls into the following categories:

- **Blocking software.** This type of software filters virtually anything on the Internet that the employer deems inappropriate for employees to access while at work. When employees type in questionable words or search inappropriate sites, which have been predetermined by the employer, not only are they prevented from entering, but they may be directed automatically to the company's electronic communications policy. The software also can alert employers when an off-limits site is visited. The main features of this software include www.cybersitter.com, www.netshepherd.com, www.xstop.com, and www.surfwatch.com.
- **Direct surveillance.** This software takes a picture of an employee's screen at periodic intervals, which enables the employer to see the sites employees are visiting or the messages they are e-mailing. An example is www.spectersoft.com.
- **Flagging.** This software not only monitors employees' Internet use but also screens their e-mail for potentially offensive or inappropriate messages. This software scans employee e-mails for questionable keywords pre-determined by the employer. For example, an employer concerned with the theft of its trade secrets can list the names of its primary competitors as keywords. This software also can automatically e-mail "flagged" messages to a company representative. An example is www.cybersitter.com.
- **Keystroke logging.** This software maintains a record of keystrokes and tracks computer idle time. This software can even recreate "deleted" documents because the keystrokes are logged and stored even if deleted. See, for example, www.adavi.com. The Program Investigator from www.winwhatwhere.com also monitors every instant message.

Electronic usage policies are effective only if utilized consistently, regularly and fairly. To reduce legal risk effectively, employers must enforce these policies consistently, without imposing undue burdens on employees or its computer staff. Ideally, the system must support time- and event-based destruction of old messages and must allow a company to halt scheduled deletion of messages selectively in order to respond to preservation orders and discovery requests. Finally, the electronic monitoring policy must be coordinated with other records management systems so that computer administrators can apply retention rules to different types of records.

CONCLUSION

- Dow Chemical fired 74 employees, including executives, and punished 435 others for distributing and viewing sexually explicit and graphically violent materials via company e-mail in 2000. One worker commented that he didn't think the e-mail "jokes" he sent were offensive because "most of the people in his department were either receiving or sending similar messages."[45]
- Xerox fired more than 40 employees for wasting up to eight hours a day surfing pornographic websites in 1999.[46]

The U.S. Supreme Court has held that "an employer can be liable [for workplace co=-worker harassment] where its own negligence is a cause of the harassment. An employer is negligent with respect to sexual harassment if it knew of or should have known about the conduct and failed to stop it. Negligence sets a minimum standard for employer liability under Title VII."[47]

Employers therefore may be considered negligent if they do not monitor their electronic workplace, just like they may be

45. Brenda Rios, *Dow's Audit of Workers' E-mail Ends in Firings*, DETROIT FREE PRESS, July 27, 2000 (online at www.freep.com/money/business/doww27_20000727.htm); *Dow Chemical Fires 50 over E-Mail Abuse*, USA TODAY, July 28, 2000 (online at www.usatoday.com/life/cyber/tech/cti298.htm); *Dow Chemical Fires Another 24 over E-Mail*, USA TODAY, September 14, 2000 (online at www.usatoday.com/life/cyber/tech/cti530.htm).

46. Bloomberg News, *Xerox Fires 40 for Online Pornography on Clock* (online at http://news.com.com/2102-1001-231058.html?legacy=cnet).

47. Burlington Indus. v. Ellerth, 524 U.S. 742, 758-59 (1998).

considered negligent for failing to monitor their physical workplace. Employers may avail themselves of the affirmative defense if they take prompt and effective remedial action to end harassment once they know or should have known of it. If the employer fails to do so, "the combined knowledge and inaction may be seen to demonstrate negligence."[48]

Another reason to monitor employee e-mail and Internet usage is to gather support for an after-acquired evidence defense to an adverse employment action. This defense generally enables an employer to avoid some (or even all) liability where it could show, after terminating an employee even for unlawful reasons, that it learned the employee previously had engaged in conduct that, if discovered, would have led to termination. With respect to federal anti-discrimination laws, the Supreme Court has held that after-acquired evidence cannot operate to bar all relief, but it can limit damages award and generally will render reinstatement and front pay inappropriate.[49]

For example, suppose a terminated employee sues for discrimination. After culling through the employee's e-mails, the employer learns that the employee was sending confidential information to competitors or pornographic e-mails to co-workers, both of which are violations of the company policies. The employer then raises the after-acquired evidence defense in reliance on this information. To be effective, the employer's electronic communications policy must specifically prohibit the usage that would subject the employee to discipline.

It is still too early to draw conclusions about what course the courts will chart on monitoring the electronic workplace. By tracking and monitoring employee usage, the employer may be storing information that might later be used against it. By not monitoring, given the prevailing notion that most workers engage in at least some form of personal use of their workplace computers, employers may be complicit in maintaining a hostile work environment.

---

48. Faragher v. City of Boca Raton, 524 U.S. 775, 789 (1998).

49. *See* McKenna v. Nashville Banner Pub. Co., 513 U.S. 352, 363 (1995) ("Where an employer seeks to rely upon after-acquired evidence of wrongdoing, it must first establish that the wrongdoing was of such severity that the employee in fact would have been terminated on those grounds alone if the employer had known of it at the time of the discharge.").

The Privacy Project

Romantic Relationships at Work: Does Privacy Trump the Dating Police?

Courts generally have upheld fraternization policies that balance employer and interests carefully and that are administered impartially

By Rebecca J. Wilson, Christine Filosa and Alex Fennel

IN TODAY'S work-oriented culture, office romances and the related topics of sex and privacy have become important issues confronted by most employers. With more employees working longer days and spending so much of their time on-the-job, romantic relationships at work are developing more frequently.[1] Workplace romance may be the only option for employees whose workload limits their outside activities; but for employers, this trend may prove problematic as the potential liability associated with these relationships rises.[2]

A 1998 survey by the Society for Human Resource Management predicted that 55 percent of office romances would likely result in marriage, but that 28 percent of these office relationships may result in complaints of favoritism from coworkers, 24 percent in sexual harassment claims, and another 24 percent in the decreased productivity of the employees involved.[3] Statistics such as these have motivated employers to adopt prophylactic policies in an effort to avoid the potentially complicated and unsavory outcomes of office affairs and to maintain a strictly professional work environment.

IADC member Rebecca J. Wilson is a partner in the Boston office of Peabody & Arnold LLP and vice chair of the litigation department, where she concentrates in employment law and works with employers to develop procedures and policies to prevent employment-related claims. She received her undergraduate degree from Trinity College in Washington, D.C., and her law degree from Boston College in 1979.

Christine Filosa, a former associate at Peabody & Arnold, is now associate legal counsel at the Education Development Center Inc.

Alex Fennel was a summer associate in 2002 at Peabody & Arnold and is a third-year law student at Boston University.

As protection from litigation and potential liability, some employers adopt policies directly addressing dating in the workplace. These policies range from the very strict, such as a comprehensive prohibition of dating between employees, to the more lenient, such as a policy that actively discourages, but ultimately allows, employees to fraternize.[4] Even a simple policy requiring employees to notify management when coworkers are romantically involved provides documentation of a consensual rela-

1. Davan Maharaj, *The Birds and the Bees—and the Workplace*, L.A. TIMES, available at http://cgi.latimes.com/class/employ/career/birdsbees991121.htm (March 1, 2002)

2. Harvey R. Meyer, *When Cupid Aims at the Workplace; Romances Between Coworkers Can Cause Problems for a Company; Be Prepared to Handle Such Situations*, NATION'S BUSINESS, available at www.findarticles.com/cf_0/m1154/n7_v86/20797623/print.jhtml (July 1998).

3. *Cupid's Arrows Sometimes Compete with Work Objectives—SHRM Survey Finds Office Romances Are Often Frowned upon by Employers*, available at www.shrm.org/press/releases/980128-3.htm (January 28, 1998).

4. Jennifer L. Dean, *Employer Regulation of Employee Personal Relationships*, 76 B.U.L. REV. 1051, 1052-53 (1996).

tionship that could be helpful to an employer's defense against a sexual harassment claim, should one arise.[5]

Perhaps daunted by problems of implementation and enforcement, other employers have avoided adopting any formal policy explicitly addressing the issue of romance in the workplace, choosing instead to rely on unwritten rules or other policies already in place. Studies indicate that some employers choose to "rely on a quiet form of persuasion . . . [b]elieving that despite having no written rules, their employees understand that as a matter of corporate culture or implied policy . . . supervisor-subordinate relationships" will be discouraged or simply not tolerated.[6]

Although employers generally enjoy the right to promulgate rules and regulations restricting dating on the job as they deem necessary, this right must be weighed against the countervailing privacy rights of their employees.[7] Courts considering these issues have balanced the employer's legitimate business interests in avoiding unnecessary litigation and potential legal liability and in maintaining a fair and professional work environment, against the privacy rights of employees.[8]

EMPLOYERS' BUSINESS INTERESTS

Many employers adopt anti-fraternization policies in an effort to avoid the numerous types of liability they might otherwise confront.[9] Liability may attach to an employer confronted with an office romance in a variety of ways.[10] First, a romantic relationship between a manager or supervisor and his or her subordinate may result in allegations of favoritism, with coworkers claiming that the subordinate has received preferential treatment as a result of the relationship. For example, the subordinate may receive longer breaks, be given preferred shifts or receive unfairly favorable reviews. Over time, this perception of favoritism could lower employee morale and productivity—two business elements that employers have a vested interest in protecting.[11]

These complaints also may trigger a sexual harassment claim against an employer under Title VII of the Civil Rights Act, 42 U.S.C. § 2000e, which enables employees to base claims of sexual harassment on, first, a "quid pro quo" argument where an employer conditions benefits, promotions or even employment itself on the receipt of sexual favors, or, second, an argument that sexual harassment has produced a hostile work environment.[12] Title VII further holds an employer vicariously liable for "actionable discrimination caused by a supervisor but subject to an affirmative defense looking to the reasonableness of the employer's conduct as well as that of the plaintiff victim," to quote the U.S. Supreme Court in *Faragher v. City of Boca Raton*.[13]

The U.S. Court of Appeals for the Fifth Circuit took guidance from the Supreme Court in *Defenbaugh-Williams v. Wal-Mart Stores* when it held that employers could be vicariously liable for sexual harassment committed by supervisors.[14] One

---

5. Gary M. Kramer, *Limited License to Fish off the Company Pier: Toward Express Employer Policies On Supervisor-subordinate Fraternization*, 22 W. NEW ENG. L. REV. 77, 143 (2002).

6. Dean, *supra* note 4, at 1053; Kramer, *supra* note 5, at 143.

7. Kramer, *supra* note 5, at 105. *Cf.* Shuman v. City of Philadelphia, 470 F.Supp. 449, 459 (E.D. Pa. 1979) (individual's private sexual activities fall within "zone of privacy" protected by Constitution so long as they do not substantially impact individual's ability to perform job).

8. Dean, *supra* note 4, at 1053.

9. Kramer, *supra* note 5, at 77-79.

10. Mary Stanton, *Courting Disaster*, from GOVERNMENT EXECUTIVE, October 1, 1998, available at www.govexec.com/features/1098/1098s4.htm (describing dating between supervisors and subordinates as "supervisory suicide"); LABOR & EMPLOYMENT IN MASSACHUSETTS: A GUIDE TO EMPLOYMENT LAWS, REGULATIONS AND PRACTICES, §§ 5-6 (Matthew Bender and Co. 2001).

11. Dean, *supra* note 4, at 1055 and n.23.

12. *Id*. at 1054. *See also* Lisa Mann, *Resolving Gender Conflict in the Workplace: Consensual and Nonconsensual Conduct*, available at website of Modrall Sperling—www.modrall.com/articles/article_44.html (October 27, 1994).

13. 524 U.S. 775, 780 (1998).

14. 188 F.3d 278, 280 (5th Cir. 1999).

of Wal-Mart's district managers stated during a meeting with other employees that a certain female, the plaintiff employee, "would never move up with the company being associated with a black man." The manager later became the plaintiff's supervisor and instituted a series of disciplinary actions against her on what she alleged were "fabricated workplace-policy grounds," which culminated in her termination. She sued on a theory of sexual harassment.

The court held that Wal-Mart was vicariously liable for the sexual harassment committed by the supervisor. Concluding that the Supreme Court intended to extend principles of agency liability to "all vicarious liability inquiries [brought] under Title VII for acts of supervisors," the court concluded that Wal-Mart was liable for damages based on evidence that the manager had acted with malice or reckless indifference by terminating the plaintiff for having been involved in an interracial relationship.

Such a ruling exposes employers to increased liability for the acts of supervisors in various contexts, which may include the enforcement of anti-fraternization policies. This strict liability under Title VII provides yet another reason for employers to implement these policies with great care and to ensure that their staff is well trained in enforcing the policies.[15]

Another danger is that while two employees are romantically involved in a consensual relationship, neither will claim harassment, but after the romance ends, one party may come forward with the contention that the association was unwelcome, even coerced. This situation presents at least two problems unique to workplace relationships between managers or supervisors and their subordinates, because of the unequal bargaining power of the parties. First, if the subordinate is disciplined, demoted or terminated, he or she may allege retaliation. Second, the party who ended the relationship may bring a sexual harassment claim based on allegations that the other party is forcing him or her to stay in the relationship, stalking or continuing to make unwanted sexual advances, thus subjecting the complainer to sexual harassment. Even if the relationship does not terminate, co-workers may attempt to make a claim against the employer for sexual harassment. That claim may be viable if the employees involved in the relationship repeatedly display sexual favoritism or other inappropriate sexual behavior in the workplace that results in the creation of a hostile work environment.[16]

Even when the relationship does not involve a manager-supervisor and a subordinate, employers still face potential litigation and liability stemming from the romance.[17] Problems can arise, for example, when an employer decides to discipline, demote or terminate a party to a workplace romance even for unrelated reasons. Employees who previously complained of sexual harassment may allege that the disciplinary action was retaliatory. That is, the employee may bring a claim against the employer.[18] They then may also bring a gender discrimination claim, alleging that the employer's action was motivated by favoritism of one gender over another.[19]

Based on this potential legal liability and a reasonable desire to maintain a productive staff, an employer has a legitimate business interest in drafting rules and regulations that will help it to avoid the myriad of problems that office romances can create.[20] For instance, if an employer prohibits its supervisors from dating their subordinates, it may be less likely to face a quid pro quo sexual harassment charge. Similarly, if a company requires its employees

---

15. Kramer, *supra* note 5, at 120; Tara Kaesebier (Comment), *Employer Liability in Supervisor Sexual Harassment Cases: The Supreme Court Finally Speaks*, 31 ARIZ. ST. L.J. 203, 223 (1999).

16. *See* for this paragraph Kramer, *supra* note 9, at 87-94; Stanton, *supra* note 10; Mann, *supra* note 12; Dean, supra note 4, at 1054.

17. Meyer, *supra* note 2.

18. Kramer, *supra* note 9, at 96.

19. *See* Sanguinetti v. United Parcel Service, 114 F.Supp.2d 1313 (S.D. Fla. 2000) (male supervisor terminated for violating employer's no-dating policy sued for gender discrimination where female manager who violated policy was not terminated).

20. Kramer, *supra* note 9, at 79.

to sign acknowledgement or consent forms when they enter into a romantic relationship with a coworker, they will have documentation on file to defend themselves from liability if a claim against them is later brought.[21] However, these rules, intended to shield employers from litigation, may, ironically, give rise to other forms of liability when an employer enforces them. When an employee is subjected to an adverse action in connection with their job for a violation of an anti-fraternization policy, the employee may challenge the employer's rules regarding employee relationships, arguing that the regulations constitute an invasion of privacy.[22]

EMPLOYEES' PRIVACY INTERESTS

At the heart of employees' interests in engaging in consensual workplace relationships lies their rights to privacy. In its original form, the constitutional right to privacy protected individuals from improper acts of government officials.[23] Since its recognition in the 1950s, however, the constitutional right to privacy has grown to encompass the autonomy individuals enjoy in making certain kinds of decisions, especially those of a particularly personal nature. Personal decisions likely to be protected by this right to privacy include issues surrounding marriage, procreation, contraception, child- rearing and education.[24] The right to privacy also protects the right of individuals to be free from governmental surveillance and intrusion in their private affairs.[25]

Every state in the United States now recognizes "some general form of common law protection for privacy."[26] Public sector employees in several states also enjoy state constitutional protection of a general privacy right.[27] Florida's Constitution limits the ability of government employers to invade the privacy of their employees.[28] Texas courts have held that the Texas Bill of Rights protects "personal privacy from unreasonable intrusion" and have extended this protection to the rights of public sector employees.[29] In California, employees may invoke a public policy exception to at-will employment termination by asserting a violation of their privacy right under the state constitution.[30]

In addition to these more conventional forms of protection, more than half the states have legislation protecting employee privacy with regard to activities conducted outside the workplace.[31] In Colorado, North Dakota and New York these laws are general enough to protect almost all legal activities not related to an individual's employment. New York's, for instance, extends quite broadly to protect the "legal recreational" activities of employees.[32] Colorado's states that it is an unfair employment practice to discriminate against

---

21. Maharaj, *supra* note 1.

22. Dean, *supra* note 4, at 1058; Kramer, *supra* note 9, at 105.

23. William M. Beaney, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212 (1963) (discussing the meaning of the constitutional right to privacy).

24. Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925) (extending constitutional right of privacy to child rearing and education); Prince v. Massachusetts, 321 U.S. 158 (1944) (extending constitutional right of privacy to decisions regarding family relationships); Skinner v. Oklahoma ex. rel. Williamson, 316 U.S. 535 (1942) (extending constitutional right of privacy to procreation); Loving v. Virginia, 388 U.S. 1 (1967) (extending constitutional right of privacy to marriage); Griswold v. Connecticut, 381 U.S. 479 (1965) (extending constitutional right of privacy to contraception); Roe v. Wade, 410 U.S. 113 (1973) (extending constitutional right of privacy to abortion).

25. Bruce L. Watson, *Disclosure of Computerized Health Care Information: Provider Privacy Rights Under Supply Side Competition*, 7 AM. J. L. AND MED. 265, 269 (1981), *citing* Roe.

26. Michael Z. Green, *A 2002 Employment Law Odyssey: The Invasion of Privacy Tort Takes Flight in the Florida Workplace*, 3 FLA. COASTAL L.J. 1, 9 (2001).

27. Helen M. Richards, *Is Employee Privacy an Oxymoron?* 15 DELAWARE LAW. 20, 20-21 (1997).

28. Green, *supra* note 26, at 14.

29. Texas State Employees Union v. Texas Dep't of Mental Health and Mental Retardation, 746 S.W.2d 203 (Tex. 1987).

30. Semore v. Pool, 1990 Cal.App. LEXIS 94.

31. Alison J. Chen (Note), *Are Consensual Relationship Agreements a Solution to Sexual Harassment in the Workplace*, 17 HOFSTRA LAB. & EMP. L.J. 165, 188 (1999).

32. N.Y. LABOR LAW § 201-d (2002).

employees for engaging in "lawful activities," either outside of the office or while working.[33] North Dakota's makes it unlawful to hire or fire an employee for engaging in a "lawful activity outside work" that does not interfere with the employer's business interests.[34]

ANTI-FRATERNIZATION POLICIES: BALANCING COMPETING INTERESTS

A. Public Sector Employees

The liberty that employers have to limit the activities of employees varies depending on whether they operate in the public or private sector. There are significant differences between these two arenas as they relate to the regulation of romantic involvement in the workplace.

State and federal constitutional provisions that explicitly protect individual privacy rights apply only to state actions.[35] When the state is the employer, it may not, without substantial justification, condition employment on the relinquishment of constitutional rights, but it nevertheless has greater latitude in restricting the activities of its employees than it has in regard to the activities of its citizens at large.[36] Accordingly, public sector employees generally enjoy a more rigorously protected right of privacy than do employees in the private sector. The courts must carefully consider both the interests of the individual and the interests of the government when determining whether the private activities of a public employee constitute valid grounds for action.[37]

Apparently aware of the intricacies of these issues, the U.S. District Court for the Eastern District of Missouri opined in *Wieland v. City of Arnold* that it was "uncomfortable" adopting a general rule that all dating relationships are constitutionally protected, especially for government employees working in "sensitive areas" of law enforcement.[38] In that case, a police officer challenged a city's police department regulation prohibiting unbecoming conduct violated, among other things, his right to privacy.

The chief of police had ordered the plaintiff to end his relationship with a woman who was on probation for a felony offense. The plaintiff had appeared at a city ribbon-cutting ceremony with the woman, and a picture of the two at the ceremony appeared in a local paper. The chief thought that this public appearance both embarrassed the city and violated a general order of the department "forbidding as unbecoming conduct . . . [k]nowingly associating, on or off duty, with convicted criminals or lawbreakers under circumstances which could bring discredit upon the department or impair an officer in the performance of his duty."

The court held that although the plaintiff's relationship with a convicted felon did not impact his job performance, it was not "unreasonable to assume a very real likelihood that it could affect the chain of command as well as the public image of the department." The court ultimately concluded that while such "looser socialties" as dating may be protected, they receive less stringent protection from privacy laws than other, more formal associations might enjoy.

In *Shawgo v. Spradlin*,[39] the Fifth Circuit specifically noted that the right to privacy does not come without qualification and that the state has a greater interest in regulating the activities of its employees than it has in regulating the activities of the general population. In *Shawgo*, two former police officers sued a city and others for an alleged invasion of privacy resulting from the disciplinary action taken against them for dating and allegedly cohabitating in violation of department regulations. One

---

33. COLO. REV. STAT. ANN. § 24-34-402.5.
34. N.D. CENT. CODE § 14-02.4-0.8 (1997).
35. Born v. Blockbuster Video Inc., 941 F.Supp. 868, 870 (S.D. Iowa 1996).
36. Briggs v. North Muskegon Police Dep't, 563 F.Supp. 585, 587 (W.D. Mich. 1983) (citations omitted).
37. Dean, *supra* note 4, at 1058; Kramer, *supra* note 9, at 106.
38. 100 F.Supp.2d 984, 988 (E.D. Mo. 2000).
39. 701 F.2d 470, 482-83 (5th Cir. 1983). 1 *Id.* at 472.

officer was a patrolwoman and the other a sergeant. The patrolwoman did not report directly to the sergeant, so the problems common to romantic relationships between managers or supervisors and their subordinates did not arise.

Finding a rational connection between the "exigencies of department discipline and [the rule] forbidding members of a quasi-military unit, especially those different in rank, to share an apartment or to cohabit" the court nevertheless concluded that the policy did not offend the plaintiffs' privacy rights. It went on to hold that the investigatory surveillance of the employees' off-duty association in violation of department regulations did not impinge upon the right to privacy.

Similar cases have reached consistent outcomes where the relationship is between a government employee and a non-government employee. For example, in *City of Sherman v. Henry*, the Texas Court of Appeals determined that a police officer's right to privacy was violated when he was denied a promotion because of a personal relationship with a fellow police officer's wife.[40] In *Briggs v. North Muskegon Police Department*, the federal district court for the Western District of Michigan applied like reasoning to conclude that a city violated a police officer's privacy rights when it dismissed him for cohabitating with a woman while separated from his wife.[41]

A police officer's right to privacy also was violated in *Shuman v. City of Philadelphia* when the police department fired him for living with a married woman who was not his wife.[42] In contrast, however, recall that *Wieland* held that a city's order to a police officer to terminate his relationship with a known felon pursuant to a policy forbidding association with a convicted criminal did not violate the police officer's right to privacy.

Since their employees possess somewhat stronger rights of privacy in the workplace than do their counterparts in the private sector, employers in the public sector should exercise caution when structuring anti-fraternization policies.[43] Relevant case law indicates that courts will evaluate anti-fraternization policies of government employers relative to the type of work involved, the existence of superior-subordinate relationships and whether one of the two employees directly reported to the other.

B. Private Sector Employees

Private sector employees receive protection from invasions of privacy under state legislation and common law. Several states have adopted laws protecting all legal off-duty activities, provided they do not directly conflict with an employer's legitimate business interest.[44] Private sector employees, however, have very few privacy rights that protect them within the workplace. To prevail on an invasion of privacy claim, there must exist a reasonable expectation of privacy in the matter at issue. Under this standard, if employees have advance notice of a company anti-fraternization rule, their claim is substantially weakened.[45] An employee who knowingly violates an anti-fraternization rule cannot be said to have had a reasonable expectation of privacy in the matter.

In *Rogers v. International Business Machines Co.*,[46] the employer dismissed a manager for having an alleged relationship with a subordinate that "exceeded normal or reasonable business associations, [and] negatively affected the duties of his employment." The employer had no policy or rule prohibiting such relationships, and the manager claimed that his termination was improper because it was predicated on an investigation of a personal matter, which invaded his right of privacy.

The U.S. District Court for the Western District of Pennsylvania concluded that the

40. 910 S.W.2d 542, 556 (Tex.App. 1995).
41. 563 F.Supp. 585 (W.D. Mich. 1983).
42. 470 F.Supp. 449 (E.D. Pa. 1979).
43. Dean, *supra* note 4, at 1058.
44. Ann H. Zgrodnik (Comment), *Smoking Discrimination: Invading an Individual's Right to Privacy in the Home and Outside the Workplace?* 21 OHIO N.U.L. REV. 1227, 1244-45 (1998).
45. Kramer, *supra* note 9, at 120, 129.
46. 500 F.Supp. 867, 868 (W.D. Pa. 1980).

employer acted reasonably, noting that nothing on the record indicated any impropriety and that in fact the manager had participated in the investigation and had received timely notice of his termination. In support of its decision, the court cited what it described as the employer's legitimate interest in "preserving harmony among its employees and . . . preserving normal operational procedures from disruption."[47] The court also rejected the plaintiffs' tort claim for invasion of privacy. It underscored the fact that the employer had limited its investigation to interviews with employees and to an examination of company records, and it concluded that the employer had not intruded on the plaintiff's "seclusion or private life."

Similarly, in *Watkins v. United Parcel Service*,[48] the employer fired a manager for violating the company's anti-fraternization policy by having a romantic relationship with a U.P.S. truck driver. The manager claimed the company's conduct was "highly offensive" because his personal relationship with the driver did not concern the company because it occurred primarily off the job. He also alleged that he and the co-worker had contemplated marriage and that his discharge prevented that marriage from coming to fruition.

The U.S. District Court for the Southern District of Mississippi rejected the claims and found at least partial support for its decision in the manager's failure to provide, or even allege, an "utterly reckless" invasion by the company, such as snooping in his bedroom or electronically wiring his workspace.

In *Patton v. J.C. Penney Co.*,[49] a former employee sued for wrongful discharge and intentional infliction of emotional distress after being terminated for dating a co-worker. One of the employer's supervisors had told the plaintiff to end his "social relationship" with a female co-worker. The plaintiff responded by saying that he did not socialize while working and that he would continue to see the co-worker during his own time. The supervisor later told the plaintiff that his job performance was not satisfactory and that he would be fired if his performance did not improve. The plaintiff employee asked to be transferred to another department, but the supervisor denied his request, and he ultimately was terminated for unsatisfactory job performance.

In affirming the lower court's judgment for the employer, the Oregon Supreme Court held that the dismissal did not violate public policy and did not amount to "outrageous" conduct.

In a similar case, *Sarsha v. Sears Roebuck & Co.*,[50] the plaintiff employee, a supervisor, was fired for dating a subordinate employee, who, however, was not fired. The plaintiff sued, alleging age discrimination in violation of the Age Discrimination in Employment Act, and a gender discrimination claim in violation of Title VII. In rejecting the claims, the Seventh Circuit ruled that the employer was "entitled to enforce a non-dating policy . . . against [its] supervisors, who by virtue of their managerial positions are expected to know better."

Nevertheless, to be upheld, an employer's anti-fraternizations policies must be enforced consistently and in a gender-neutral manner. For instance, in *Zentiska v. Pooler Motel Ltd.*,[51] the employer ordered one of its supervisors either to quit his job or fire the plaintiff employee the supervisor was dating. The supervisor removed the plaintiff employee's name from the work schedule. One of the employer's area directors, however, had dated and ultimately married a co-worker. The employer had not enforced its anti-fraternization policy with respect to that situation. The area director not penalized was male; the plaintiff who was fired was female. The federal district court in Georgia found the defendant liable for sex discrimination on the ground that it had treated the female plaintiff differently from a similarly situ-

47. *Quoting* Geary v. U.S. Steel Corp., 319 A.2d 174, 178 (Pa. 1974).
48. 797 F.Supp. 1349, 1351 (S.D. Miss. 1992).
49. 719 P.2d 854 (Or. 1986).
50. 3 F.3d 1035, 1037 (7th Cir. 1993).
51. 708 F.Supp. 1321, 1322-25 (S.D. Ga. 1988).

ated male employee.

Courts that have encountered these issues have consistently decided in favor of the proposition that employers must act reasonably and consistently, both in the implementation and the execution of anti-fraternization policies.[52] For instance, in *Watkins*, the plaintiff did not argue that the anti-fraternization policy itself constituted an invasion of privacy, but rather that the investigation into the relationship violated his privacy rights. As that case demonstrates, the manner in which a company enforces its anti-fraternization policy is equally important to an employer seeking to avoid litigation as the policy itself.

Employers who adopt anti-fraternization policies appear to be fairly well protected from liability on invasion of privacy grounds, so long as the policy and its implementation are reasonable.[53] Courts have demonstrated sympathy for the plight of employers facing problems arising from fraternization between employees. They recognize that workplace romances can have a tangible and often negative impact on a company's ability to achieve legitimate business objectives. At the same time, however, courts maintain a clear respect for the individual privacy rights of employees and will not allow those rights to be abrogated beyond reason.[54]

To arm themselves against various kinds of liability, employers should craft policies that are reasonable in scope and degree and that can be fairly and consistently enforced. A reasonable policy will focus on the effect the relationship has on the business interests of the employer. For example, there should be some correlation between the romantic relationship and the employees' performance on the job. It likely will be more difficult to defend an anti-fraternization policy relating to the activities of employees outside the workplace if the policy does not require that the outside activity impact a legitimate business objective or interest.

C. Off-duty Conduct

Another important issue that arises in cases involving romantic relationships at work centers around the highly controversial idea that employers have the ability and also the right to regulate the activities of their employees outside the workplace. The best-known case on this issue involves two former employees of Wal-Mart, *New York v. Wal-Mart Stores*.[55] Both were terminated for violating the company's fraternization policy, which prohibited a "dating relationship" between a married employee and another employee, other than his or her own spouse.

In an action seeking the re-instatement of the terminated employees, the New York Attorney General argued that the firing violated a New York statute that made it unlawful for any employer to "refuse to hire, employ, or license or to discharge from employment or otherwise discriminate against an individual . . . because of . . . an individual's legal recreational activities outside work hours, off the employer's premises and without use of the employer's equipment or property."[56]

The outcomes of cases interpreting this statute have hinged almost entirely on the courts' interpretation of the phrase "recreational activities." In the *Wal-Mart* case, the trial court had found that the employees may have engaged in recreational activities while dating and that the fact that they engaged in these "protected leisure activities . . . together did not vitiate their statutory protection." The Appellate Division, however, reversed, holding that "dating" is distinct from and, in fact, bears no resemblance to "recreational activity." The employees could not receive protection under the statute.

Critics of the court's reasoning, however, have argued that this interpretation of

---

52. *See* Sanguinetti v. United Parcel Serv., 114 F.Supp.2d 1313 (S.D. N.Y. 2000) (dismissing invasion of privacy claim brought by employee fired for violating no-dating rule).

53. Kramer, *supra* note 9, at 78, 96.

54. Michael Dworkin, *It's My Life—Leave Me Alone: Off-the-Job Employee Associational Privacy Rights*, 35 AM. BUS. L.J. 47, 95 (1997).

55. 621 N.Y.S.2d 158 (App.Div. 3d Dep't 1995).

56. N.Y. LABOR LAW § 201-d.

the statute "overlooks [its] essential purpose, which is to protect employees' off-the-job activities so long as they [do not bear]" on one's job performance.[57] In contrast, a New York federal district court's interpretation of the same language concluded that cohabitation qualified as a recreational activity under the statutory scheme.[58] The court relied on the statute's legislative history, which it held reflected a "general policy of protecting employees from discrimination" against employees who happen to engage in activities after work that their employer does not like.

Many states have adopted these off-the-job privacy laws in some shape or form, indicating that this type of statute will remain a force to be reckoned with as employers confront the issue of romantic relationships in the workplace and draft anti-fraternization policies.[59] Ultimately, it appears that the outcome of these cases will depend on the legislative history of the statutes involved and how courts decide to interpret the relevant statutory language.

D. Privacy on the Internet

Another related issue is whether employees have an expectation of privacy with regard to e-mails sent or received on an office computer system. For instance, an employer might discover that its employees are fraternizing in violation of a company policy by intercepting a related e-mail message. In *Restuccia v. Burk Technology Inc.*,[60] the Massachusetts Superior Court held in 1996 that employees do not have a reasonable expectation of privacy regarding e-mails sent and received at work and that, therefore, an employer did not violate the state wiretapping law when it stored and reviewed messages from a company server.

More recently, the U.S. District Court for the District of Massachusetts held that even where employees may have a reasonable expectation of privacy in their office e-mail, the legitimate business interests of their employers will likely trump employee privacy interests. In *Garrity v. John Hancock Mutual Life Insurance Co.*,[61] that court noted that both Title VII and state law require employers take proactive steps to eliminate harassment from their offices and to investigate any potentially harassing conduct when this conduct is brought to their attention.

Similarly, in *Smyth v. Pillsbury Co.*,[62] the federal district court in the Eastern District of Pennsylvania held that pursuant to Pennsylvania law, an employee fired for making disparaging comments on an e-mail written at work did not have an expectation of privacy in this communication. In *McLauren v. Microsoft Corp.*[63] a Texas Court of Appeals held that an employee did not have a reasonable expectation of privacy in the contents of an e-mail message that he had saved to a "personal" file.

Thus, it appears that an employer who discovers a violation of its fraternization policy by intercepting an e-mail sent on an office system does not violate the privacy rights of the employees involved in acting on knowledge acquired via the intercepted message.

CRAFTING ANTI-FRATERNIZATION POLICIES

A well-drafted, carefully implemented and widely disseminated corporate policy regarding fraternization among employees can provide substantial legal protection to employers.[64] The employer must first determine the nature of the limitation desired and then decide how it will enforce the policy. The policy should provide a precise definition of the discouraged, limited or

---

57. Dworkin, *supra* note 54, at 53-54.
58. Pasch v. Katz Media Corp., 1995 WL 469710 (S.D. N.Y.).
59. Dworkin, *supra* note 54, at 55; Dean, *supra* note 4, at 1067 nn. 114-115.
60. 1996 Mass.Super. Lexis 367 (1996).
61. 2002 U.S.Dist. Lexis 8343 (D. Mass.).
62. 914 F.Supp. 97, 101 n.3 (E.D. Pa. 1996).
63. No. 05-97-00824-CV (Tex.App. 1999), unpublished but available at http://www.5thcoa.courts.state.tx.us/cgi-bin/as_web.exe?c05_99.ask+D+10706510.
64. For references to this section, *see* Kramer, *supra* note 9, at 78, 120; Dean, *supra* note 4, at 1073; Meyer, *supra* note 2.

prohibited conduct. For example, an employer may define the phrase "personal relationships" to encompass romantic relationships as well as family relationships or relationships with the potential for conflicts of interest.

The employer also must determine the extent to which the policy will limit such relationships. One might choose to adopt a comprehensive policy prohibiting all relationships between co-workers. Another, believing this too restrictive, might opt to limit the prohibition to personal relationships between a manager and a subordinate, with or without providing various other qualifications such as whether the subordinate reports directly to the supervisor. An even less restrictive option would be a limitation on a manager's ability to have a "personal relationship" with a subordinate within his or her chain of command.

Finally, the employer must consider the types of consequences it will apply to employees who violate the policy. These may include transfers to another department, termination, reprimand or demotion. Employers should carefully consider not only the potential reaction of its employees to the policy, but also the practicality and difficulty of enforcing it, given its business circumstances. In the end, for an anti-fraternization policy to survive claims brought on privacy grounds it must strike a reasonable balance between the interests of the employer and the interests of the employees.

An employer or advising attorney wishing to avoid claims that a policy violates the privacy rights of its employees should structure the policy around the impact potential romantic relationships at work may have on job performance. This will increase the likelihood that a court will find a rational connection between the policy and the achievement of legitimate business objectives. The more specific the policy is in defining its prohibitions and the scope of their application, the more notice employees will be seen to have had. The more notice employees have regarding their employer's anti-fraternization policy, the weaker their argument that they had a reasonable expectation of privacy regarding the romantic relationship.

An advising attorney drafting a policy should pay close attention to any guidance offered by the courts in the applicable jurisdiction and, given the uncertainty of the law in this area, should craft the policy in light of the factors that these courts have found persuasive. Employers also should ensure that the policy is clearly conveyed to all employees and understood by all employees.

At the end of this article are two sample fraternization policies.

CONCLUSION

The privacy rights of employees typically do not prohibit employers from acting as the dating police by implementing or enforcing a policy against romantic relationships in the workplace. In many, if not most instances, the employer's legitimate business interests in maintaining a peaceful and productive work environment and avoiding liability outweigh an employee's right to privacy. This has proved to be especially true in the context of an employment relationship in the private sector.

If an employer decides to promulgate rules and regulations regarding office romances, the policy should not intrude on employees' private affairs unreasonably and should display respect for the personal lives of employees, while also protecting the employer's interest in avoiding the many problems that can result from these romances. The policy should be stated clearly and tailored narrowly to protect the employer's legitimate business interests. Consideration may be given to restricting only relationships between supervisors and subordinates since in the past these relationships have been the most likely to lead to litigation because of the imbalance of power between the two parties, as well as being the most likely to affect job performance. Most critically, whatever form of policy an employer chooses to adopt, it must enforce the policy in a uniform and non-discriminatory manner.

SAMPLE ANTI-FRATERNIZATION POLICIES

Following are sample policies that employers may find helpful when drafting their own fraternization rules. Please note, however, that these are only suggested models. Employers should tailor their specific policies to the needs of their business and should get legal advice regarding the legal climate in this area of employment law within their jurisdictions.

NO FRATERNIZATION POLICY

XYZ Company Inc. prohibits supervisors or managers from engaging in romantic relationships with their subordinates within the company. Relationships between management personnel and employees raise issues of equity, fairness, favoritism and potential legal liability for the company and, therefore, will not be permitted. If management becomes aware of any such relationship, both parties will be confronted and unless they are willing to terminate the relationship, management will ask the supervisor to leave the company.

This policy does not apply to employees not in management. If, however, a relationship not covered by this policy causes disruption within the workplace or any other performance problems, discipline may be imposed.

DISCLOSURE OF CONSENSUAL RELATIONSHIP POLICY

XYZ Company Inc. requires that any employee who becomes involved in a romantic relationship with another employee of the company to report this relationship to Ms. Need T. Know, Director of Human Resources. Employees of XYZ Company Inc. who choose to engage in a romantic relationship with a co-worker are required to sign a statement that they have chosen to do so voluntarily and that as such, the relationship is consensual.

The Privacy Project

Privacy Issues from the Judicial Perspective: Requirements for Protective Orders

The frequency with which courts employ protective orders should influence counsel to draft the application with detailed statements

By Mark D. Fox and Chris E. Forte

IN THE context of litigation, the anticipated threshold issue—should the court require disclosure to an adversary of private or sensitive information—most often becomes how and to whom the court will permit disclosure of that information. Practitioners may need to explain to clients the breach of privacy consequences of raising certain issues in a lawsuit, particularly with respect to damages. They also should be aware of the necessity of raising privacy issues early in the proceedings so as to avoid a waiver.

MANDATORY DISCLOSURE AND PROTECTIVE ORDERS

In the United States, concerns may arise from a consideration of the mandatory disclosure requirements of Rule 16(a)(1)(A) and (B) of the Federal Rules of Civil Procedure, which, within 14 days of the Rule 26(f) scheduling conference require disclosure of the identities of witnesses and documents "that the disclosing party may use to support its claims or defenses." There are exceptions to the disclosure requirement, but absent a stipulation between the parties, the prudent practitioner should act to avoid the potential for preclusion pursuant to Rule 37(c)(1) by bringing any objections to the attention of the court before the Rule 26(f) conference or by stating the objection in the Rule 26(f) discovery plan.

Parties with privacy concerns about the contents of material required to be produced as part of mandatory initial disclosure also should consider the impact of the amendment to Rule 5(d), which now excludes from the requirement of filing with the clerk (and thereby renders unavailable to the public) disclosures made under Rule 26(a)(1) and (2) until they are used in the proceeding or filing is ordered by the court. Once such discovery materials are used in the action, for example, as an exhibit in support of a motion, they may become available to the public. For that reason, protective orders entered under Rule 26(c) are becoming more routine.

An April 1996 study by the Federal Judicial Center, *Protective Order Activity in Three Federal Judicial Districts, Report to the Advisory Committee on Civil Rules*, by Elizabeth C. Wiggins, Melissa J. Pecherska and George Cort, revealed that in the District of Columbia in 1990 through 1992, protective order activity occurred in between 8 and 10 percent of all the civil cases on the docket. While the numbers were lower (approximately 5 percent) in the other districts studied, the number of cases affected was still significant. The authors' experience in the Southern District of New York confirms the findings in the three districts in the study that of all appli-

Since 1991, Mark D. Fox has been a magistrate judge in the U.S. District Court for the Southern District of New York, White Plains. He is a 1967 graduate of Brooklyn Law School and a member of the New York bar since 1968.

A career law clerk, Chris E. Forte is a 1980 graduate of the State University of New York at Buffalo Law School and a member of the New York bar since 1981.

cations for protective orders between 17 and 26 percent are submitted by stipulation of the parties.

APPLICATIONS FOR PROTECTIVE ORDERS

A. General Provisions

The frequency with which courts employ protective orders should influence counsel to draft the application with a detailed statement of:

- the categories of information that would be subject to the order;
- the procedures proposed for determining which information falls within the protected categories;
- the procedure for designating material subject to the order;
- the persons who may have access to the material protected by the order;
- the extent to which protected materials may be used in related litigation;
- the procedures for maintaining security;
- the procedures for challenging particular claims of confidentiality;
- the exceptions, if any, to the order's general prohibitions against disclosure;
- the termination of the order after the conclusion of the litigation or at another time;
- the return or destruction of materials received pursuant to the order; and
- the court's authority to modify the order, both during and after the conclusion of the litigation.[1]

The provisions of the Federal Rules of Civil Procedure governing the issuance of protective orders are in Rule 26(c) and were formulated to deter any improper use of the broad range of discovery options authorized by the Federal Rules.

Rule 402 of the Federal Rules of Evidence provides in substance that all relevant evidence is admissible except as otherwise provided by law, and that evidence which is not relevant is not admiss ible. Under Evidence Rule 401:

> "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

The relevance of evidence, however, is not the yardstick by which a court measures privacy concerns. Rule 26(b)(1) broadens the scope of potential disclosures as follows:

> Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party. . . . Relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

Rule 26(c) potentially narrows the scope of disclosure by authorizing the court, for good cause shown, to enter any order which justice requires to protect a party or person from annoyance, embarrassment, oppression or undue burden or expense. The options, which are not exclusive, include:

1. Precluding the discovery.

2. Specifying the terms and conditions of the discovery. For example, in cases that involve incarcerated plaintiffs, courts, largely as a housekeeping matter, often have directed that a deposition be conducted by telephone conference call or solely on written questions. The same considerations may apply when the witness is located at a distance that does not justify the travel expense of attorneys.

Courts also may adjourn ongoing discovery proceedings to the courthouse, not merely to maintain control over obstreperous lawyers, the most common reason, but to even the playing field. In one case, a relatively small municipal police department wanted depositions of armed and uniformed defendant-officers conducted at the precinct so that coverage could be maintained. The plaintiff complained that he felt intimidated by the presence of the guns in the deposition room, so the depositions were adjourned to the federal courthouse, where all those who enter are required to check weapons at the door.

---

1. MANUAL FOR COMPLEX LITIGATION (THIRD) at 67-69 (Federal Judicial Center 1995).

3. Specifying and limiting the means or methods of discovery. For example, unless the court orders otherwise, Local Rule 33.3 of the Southern District of New York restricts the categories of information that may be the subject of interrogatories at the beginning of discovery to the names of witnesses with knowledge of information relevant to the subject matter of the action, the computation of each category of damage alleged, and the existence, custodian, location and general description of relevant documents or information of a similar nature.

4. Limiting the scope of discovery to specified matters and excluding inquiry into others.

5. Limiting the persons present during the taking of discovery. Issues in this area abound. In almost every case involving expert evidence, counsel want their expert present at most depositions and especially at the deposition of the opposing expert.

6. Opening of sealed depositions only on order of the court.

7. Limiting or specifying how trade secret or other confidential research, development or commercial information will be revealed. When commercially valuable information is in issue, as in cases of alleged theft of trade secrets, courts often appoint an independent expert to examine the formula or process of each side's product and render an opinion. This procedure protects each party's confidential material from the other.

8. The simultaneous filing of specified documents in sealed envelopes to be opened only as directed by the court.

In fashioning a protective order, or indeed in determining whether to enter one, the court will balance the movant's legitimate concerns about confidentiality against the needs of the litigation, protecting individual privacy or the commercial value of the information, while making it available for legitimate litigation use.[2]

B. Sensitive Health Information

Applications for protective orders often are made by parties who seek to avoid requested disclosure. For example, plaintiffs who allege physical injuries caused by a defendant have placed their medical conditions in issue and thereby have waived the privilege and privacy rights concerning medical records and information that otherwise might have shielded the records from disclosure. When a plaintiff seeks recovery for emotional distress and the costs of psychiatric and other mental health treatment alleged to have been necessitated by the action of a defendant, that defendant often demands all records of all treatment the plaintiff may have received. The demand may reach back for many years or even the plaintiff's entire life.

In support of the demand, the defendant asserts that some prior incident of psychiatric trauma, and not the alleged act or omission, may have caused the injury. Typically, the plaintiff will oppose the demands because the treatment was too remote in time to be relevant. On an in camera review, the court usually lacks the expertise in the field of mental health to determine the relevance of the requested information or whether it is likely to lead to admissible evidence.

While a court may conclude that plaintiffs have placed their entire mental health history in issue merely by suing, a more thoughtful approach recognizes that what has actually been placed in issue is information about the injuries that are alleged to have resulted from the defendant's act or acts and the related treatment. Of course, the defendant is entitled to explore other causes of the claimed injuries, while plaintiffs have the right to maintain the confidentiality of unrelated conditions and treatment.

A helpful solution, one that balances these competing interests, permits defense counsel and a retained expert in the field of mental health to examine the plaintiff's records under a confidentiality order that initially limits disclosure to counsel and the expert, and that specifically precludes them from disclosing any of the information to

2. *Id.* at 69.

anyone, including the client, without a further order of the court. Neither may use nor copy any of the information for any purpose except to evaluate its relevance to the issues in the litigation.

After that evaluation defense counsel will advise plaintiff's counsel if any information in the contested records has been deemed relevant to the litigation. If the information is deemed relevant, and if the plaintiff's counsel, after having consulted its own expert, disagrees, the court will conduct a hearing, take the testimony of both experts and determine the issue. This procedure protects both the plaintiff's right to privacy in unrelated information and the defendant's right to explore other causes of the alleged injuries.

The situation changes when a non-party asserts a privacy interest. In that circumstance, the court should require that notice be provided to the interested individual or entities whose privacy interests may be compromised by disclosure.

In a form approved by the court, the notice should provide basic information about the nature of the litigation, the parties, the relief sought in the lawsuit, the information sought that affects the non-party's privacy rights and information about how to convey, by telephone or in writing, the non-party's position concerning disclosure. It should also set a date when the non-party may appear in person to express directly its view concerning disclosure so as to assist the court in balancing privacy concerns against the need for disclosure.

Counsel for a party seeking such disclosure should limit the scope of the information sought to that necessary to pursue any claim or defense in the litigation, and no more. The more circumspect the intrusion into privacy rights, the less likely the protest from the non-party. Absence of response from a non-party increases the likelihood that the court will order the discovery. The key, therefore, is to evaluate carefully exactly what information is necessary and relevant for the litigant's purposes and to explore means of providing it to the parties, while protecting all other information from disclosure.

For example, in a recent case before the authors, a plaintiff, who was employed as a social worker at a medical facility, alleged that she had been terminated in retaliation for her complaints that patients in certain diagnostic categories were being transferred to nursing homes without their consent and without the appointment of committees as required by New York law.[3]

The information genuinely relevant to the issues in the suit was the existence and diagnoses of the patients on which the plaintiff was relying as the factual predicate for her allegations of retaliation. Disclosure of the actual identities of those patients was neither necessary nor desirable. The parties, with some assistance from the court, agreed to a method for separating the needed information while maintaining the confidential aspect of the records.

Counsel for the defendant medical facility created a list of the names of the patients affected and their diagnoses. The plaintiff's counsel then inspected the files under a "counsel's-eyes-only" confidentiality order to verify that all the patients known by his client to have been the subject of her complaints were included. Each patient was then assigned a code number, and all identifying data was redacted from the documents that were to be used in the litigation. The court was provided, in camera, with both the patient list and the identifying code numbers.

Counsel then stipulated to identify patients during the depositions and at trial by code number only. With the cooperation of counsel, the litigants had full access to all required information, while the privacy rights of the patients were protected.

C. Statutory Considerations

In some cases, a statute controls the terms of disclosure. The Family Education

3. The decision in this matter and others mentioned in this discussion were set forth in an unpublished order or orally on the record, a procedure which facilitates the disposition of discovery disputes and efficient case administration. Unfortunately, oral rulings on the record complicate counsel's search for specific precedent.

Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232(g), also known as the Buckley/Pell Amendment, which creates no right to sue for unauthorized disclosure,[4] allows access by parents to the school records of their children in order to challenge entries in those records but restricts third-party access absent consent of the parents or of the student, if the student is over the age of 18. FERPA's provisions do not create a bar to disclosure, but they allow an education institution to release records and information only in compliance with a validly issued subpoena or a court order and only after notification to the parents and students whose records are to be disclosed. A school district that fails to comply with the provisions of FERPA by enforcing standards relating to access to educational records may jeopardize its federally funded programs.

All of the previously discussed concerns regarding the limiting of the scope of disclosure apply and should be considered in seeking such disclosure. In considering FERPA applications, the court will balance the need of the requesting party for the information against the privacy interests of the student. In cases in which information concerning the test scores of large numbers of students may be relevant, counsel should consider a summary, chart or calculation reflecting the information. A summary, admissible under Federal Evidence Rule 1006, provides the necessary information without disclosing the identities of individuals. While the rule requires that the files or documents summarized be made available to the adverse party, stipulations or a confidentiality order tailored to the needs of the particular situation may be appropriate.[5]

ENSURING PRIVACY

A. General

Given their relatively high immutability, counsel should ensure that the client and all personnel in counsel's office understand the specific terms of any protective order and that everyone maintains full compliance with both the letter and the spirit of the order. In *Securities and Exchange Commission v. TheStreet.com*,[6] the U.S. Court of Appeals for the Second Circuit affirmed a decision in which Judge Rakoff of the Southern District of New York had unsealed portions of depositions previously designated as confidential by the parties in a so-ordered stipulation. Judge Rakoff found that the presence at the depositions of interested third parties who had not consented to the stipulation waived any claim to the confidentiality of the material. Nevertheless, the particularly sensitive nature of the information in the deposition, which concerned an allegedly illegal stock trading scheme, warranted a new protective order.

When the plaintiff, TheStreet.com, an online business news service, applied for access to the information, Judge Rakoff found that the media (and thus the public's) interest in disclosure outweighed the risk of harm that the disclosure might cause and granted the motion for access. While the Second Circuit recognized the strong presumption that protective orders will remain in force, with the exception of the presumption of access to the narrow category of "judicial documents" established in *United States v. Amodeo*,[7] it also recognized that the public should not be denied access to documents filed with the court that are relevant to the performance of the court's judicial function.[8]

Accordingly, courts should weigh the significance of the material in issue against the risk of harm to the privacy interest of those opposing disclosure. In determining applications to modify a protective order, courts will balance the continuing need for enforcement of the order and the continuity

---

4. Gonzaga University v. Doe, 122 S.Ct. 2268 (2002), *rev'g and remanding* 24 P.3d 390 (Wash. 2001), *decision below*, 992 P.2d 545 (Wash.App. 2000).

5. *See* Zayre Corp. v. S.M. & R. Co., 882 F.2d 1145, 1149 (7th Cir. 1989); Colorado v. McDonald, 15 P.3d 788 (Colo.App. 2000).

6. 273 F.3d 222 (2d Cir. 2001).

7. 44 F.3d 141, 145 (2d Cir. 1995).

8. *See* Michael C. Silverberg, *Federal Discovery*, N.Y. L.J., January 3, 2002, at 3, for a thorough and enlightening discussion of the case.

of the necessity for it against whatever factors warrant its discontinuance.

B. Sanctions

Courts' efforts to ensure that private information remains relatively undisclosed would be futile if not for the availability of sanctions, the range of which is set forth in Civil Practice Rule 37.[9] Significantly, Rule 37(a)(3) provides that "an evasive or incomplete disclosure, answer or response is to be treated as a failure to disclose, answer or respond." Under Rule 37(a)(4), on a motion to compel discovery, the court may order full disclosure and award reasonable attorney's fees and expenses to either side, depending on the outcome of the motion. In response to non-compliance the court should impose the least harsh or serious sanction commensurate with the recalcitrance and designed primarily to bring about or influence compliance.

Rule 37(b)(2) provides the following non-exclusive list:

- the subject information or other designated facts will be deemed established;
- preclude the offending party from opposing or supporting designated claims or defenses or introducing designated matters into evidence;
- strike pleadings or parts of pleadings, dismiss the action or parts of it, enter a default judgment, or stay all proceedings until compliance with the discovery order has been accomplished;
- impose contempt for failure to obey a court order except an order to submit to a physical or mental examination.

In *Drought v. Parisi*,[10] I addressed a troubling violation of a confidentiality order. An adolescent (minor) plaintiff's claims for alleged violations of his federal civil rights arose from a direction by the probation department of a state court to submit to an evaluation by penile plethysmograph at a sexual behavior clinic. The device measures and records the subject's reaction to erotic stimulus.

Pursuant to a stipulated confidentiality order, which forbade any copying or inspection of these materials outside the lawsuit, the plaintiff's counsel obtained files of other clients that had been referred to the clinic. About six months after the stipulation and during a taped segment of a local news broadcast, a reporter displayed on camera some of the material furnished pursuant to the stipulation. The plaintiff's counsel offered an assortment of after-the-fact and unpersuasive excuses, the least of which may have been that identifying information about the clients had been redacted from the files before the reporter saw them. None of the excuses justified the breach of confidentiality.

The court reminded the plaintiff's counsel of the following principle, which no litigator should forget: "When counsel willingly accedes to the entry of a stipulated protective order, the court will be hesitant to relieve that party of its obligations, particularly when the other party produced discovery in reliance on their agreement."[11] The sanctions were a fine payable to the court, a sum payable to the defendants' attorney for having had to bring the application, a direction to return all the originals and copies to defense counsel and a limitation on future access to confidential records only during regular business hours at the clinic's office. There was no appeal.

Although ultimately the district judge assigned to *Drought* dismissed the case on summary judgment, the incident concerning the violation of the confidentiality order illustrates the options and flexibility available to a court. Noteworthy, however, despite the egregious nature of the violation, a preclusion order was not issued, and no claims were dismissed.

Violations of a confidentiality order or other unauthorized revelations of private or

---

9. Lest the obvious be overlooked, he who has already revealed publicly information similar to that revealed in violation of a confidentiality order will have no cause for complaint. *See* Gordy Co. v. Mary Jane Girls, Inc., 1989 Westlaw 28477, at *7-*8 (U.S.D.C. S.D. N.Y.).

10. 92 Civ. 2188 (GLG)(MDF), U.S.D.C. S.D. N.Y., January 24, 1994.

11. Parkway Gallery Furniture Inc. v. Kittinger/ Pennsylvania House Group Inc. 121 F.R.D. 264, 267 (M.D. N.C. 1988).

sensitive information may result in the infliction of significant harm or injury. Despite the current era of reality television, the average male adolescent would undoubtedly be mortified to learn that the mere fact of his examination by penile plethysmography, let alone his arousal pattern, had been broadcast on television. To be sure, that event did not occur, but what if it had? More significantly, what if information of an intensely personal, intimate and individual nature were revealed without justification or authorization, and the revelation resulted in serious consequences?

C. Public Policy

A fundamental function of the judiciary in our society is to preserve and protect the rights and interests of individuals and entities. Research developments in the area of genetics and the human genome have led to the extrapolation that information encoded on DNA provides previously unknown revelations about how stimuli may affect an individual. Although this information has extraordinary commercial potential, an individual who produces the DNA may wish to preserve the integrity and secrecy of true identity, so to speak, to avoid being the victim of embarrassment, a stereotype, or the scientific trend of the era.[12]

In many circumstances, society has an obligation to preserve that choice through the enactment of public policy forbidding or limiting disclosures of information.[13] Apart from public policy enactments, however, should the common law provide recourse for the victims of errant disclosers? For a creative plaintiff's attorney with a case that compels the granting of relief, the answer may be that it should and that it already does. A suggestion follows for the pleading of a cause of action for the wrongful disclosure of private genetic information.

1. Federal

From the federal perspective, neither the federal courts nor Congress is likely to recognize this claim. As the U.S. Supreme Court has observed, through Justice and now Chief Justice Rehnquist: "While there is no 'right of privacy' found in any specific guarantee of the Constitution, the Court has recognized that 'zones of privacy' may be created by more specific constitutional guarantees and thereby impose limits upon government power."[14]

While Congress may regulate the distribution of private information pursuant to its power to regulate interstate commerce[15] or as part of its power to regulate the conduct of the federal government,[16] the federal courts have relied on the Fourth Amendment[17] and the due process clause of the 14th Amendment to find limitations on governmental power to affect private matters.

The Supreme Court stated in *Whalen v. Roe:*

---

12. *See* Taylor v. Kurapati, 600 N.W.2d 670 (Mich.App. 1999) (discussing the potential social consequences of information derived from DNA analysis); Rhode Island v. Morel, 676 A.2d 1347, 1356 (R.I. 1996).

13. *E.g.*, N.Y. PUB. HEALTH LAW § 2780 *et seq.* (HIV and AIDS related information); N.Y. PUB. OFF. LAW § 91 et seq. (Personal Privacy Protection Law).

14. Paul v. Davis, 424 U.S. 693, 712-13 (1976), *accord* Katz v. United States, 389 U.S. 347, 350-51 (1967); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (stating "various [constitutional] guarantees create zones of privacy").

In Gibson v. Mathews, 926 F.2d 532, 537 (6th Cir. 1991), the Sixth Circuit stated that the language of the Ninth Amendment, "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people" does not confer "substantive rights in addition to those conferred by other portions of our governing law. The Ninth Amendment 'was added to the Bill of Rights to ensure that the maxim *expressio unius est exclusio alterius* would not be used at a later time to deny fundamental rights merely because they were not specifically enumerated in the Constitution.'"

15. *E.g.*, Reno v. Condon, 528 U.S. 141, 148-49 (2000) (Driver's Privacy Protection Act of 1994).

16. *E.g.*, 5 U.S.C. § 552(b)(6) (Freedom of Information Act does not apply to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy").

17. *E.g.*, Chandler v. Miller, 520 U.S. 305, 313 (1997).

> The cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.[18]

It is ironic that if Congress were to rely on Section 1 of the 14th Amendment as authority to create a cause of action for violating federal public policy concerning a state's handling or disclosure of private information, in the absence of a waiver, the effort would probably be stymied by the state's 11th Amendment immunity from suit in federal court.[19] Similarly, the recognition of an individual's interest in nondisclosure is likely to evaporate in a scheme that balances the government's interest in disseminating the information against the individual's interest in keeping the genetic profile private.[20]

The limited reach of the federal zone of privacy compels the practitioner to look elsewhere for a theory of recovery.

2. State

Some state constitutions specifically acknowledge a citizen's right to privacy.[21] Other states have found privacy rights from the body of existing law, which includes the state's statutory and constitutional provisions.[22] With respect to a limitation on legislative power, a state constitution's specific recognition of privacy has subjected enactments to "strict scrutiny."[23]

In California, the same recognition has spawned a cause of action similar in pleading and proof to a federal claim of employment discrimination premised on Title VII. The plaintiff must establish a legally protected privacy interest, a reasonable expectation of privacy in the circumstances and conduct that constitutes a serious invasion of privacy. The defendant may negate any of these elements, or as an affirmative defense may demonstrate that the invasion is justified because it substantively furthers one or more countervailing interests. If the defendant succeeds, the plaintiff then may rebut the countervailing interest by showing that feasible and effective alternatives have a lesser impact on the privacy interest.[24]

As these examples illustrate, state courts have experience in handling and analyzing privacy claims premised on state constitutional law. Constitutional provisions, however, usually authorize or limit the power of government and its agencies. They do not restrict the conduct of non-governmental individuals and entities involved in the collection of samples and their DNA analyses and the disclosure or nondisclosure of the results. Like any interest group, those involved in this enterprise or industry may organize to lobby the state legislature so as to affect or even thwart the enactment of

---

18. 429 U.S. 589, 598-99 (1977) (footnotes omitted), *rev'g* 403 F.Supp. 931 (S.D. N.Y. 1975). For earlier proceedings below, *see* 480 F.2d 102 (2d Cir. 1973), *rev'g* 357 F.Supp. 1217 (S.D. N.Y. 1973).

19. *See* Kimel v. Florida Bd. of Regents, 528 U.S. 62, 81 (2000).

20. *See* Roe v. Marcotte, 193 F.3d 72, 80 (2d Cir. 1999); *cf.* Powell v. Schriver, 175 F.3d 107, 111 (2d Cir. 1999) (interest in privacy of medical information contained in record will vary with condition).

These cases and Schlicher v. (NFN) Peters I & I, 103 F.3d 940 (10th Cir. 1996), involve the state's use of individuals in custody to establish a DNA data bank to deal more effectively with recidivism. Courts allow the collection of this information because the governmental interest in solving crime efficiently is legitimate and the intrusion to obtain the DNA is minimal. These cases raise an issue that has not been addressed judicially: Should an individual, who apparently has lost the right to privacy by virtue of having committed a crime, nevertheless be able to regain it after the proverbial debt to society has been paid?

21. *E.g.*, CAL. CONST. Art. I § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . privacy."); MONT. CONST. Art. II § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); WASH. CONST. Art. I § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.")

22. *See, e.g.*, Jegley v. Picado, 80 S.W.3d 332 (Ark. 2002).

23. Gryczan v. Montana, 942 P.2d 112, 122 (1997) (legislation must be justified by compelling state interest and must be narrowly tailored to effectuate only that compelling interest).

24. Am. Academy of Pediatrics v. Lungren, 940 P.2d 797, 811 (Cal. 1997).

public policy that would regulate their activities. Given the formalities of the process of judicial review, organized lobbying has far less impact on a lawsuit grounded in a common law cause of action.

D. Framework for a Remedy

The potential application of the results of an individual's DNA analysis requires a framework that protects one from commercial exploitation and respects the preference for maintaining privacy.

Traditional "privacy" torts were developed before our level of knowledge about the human genome. With the exception of the public disclosure of private facts, those torts focus on commercial exploitation. In New York state, statutory enactments have limited their scope in a manner that does not favor an analogy between the rights protected by the statutes and an individual's interest in maintaining the privacy of DNA information.[25] The concepts of property involved in commercial exploitation also limit the reach of the tort of conversion.

For instance, in a California case, although the result may be fact specific, the allegations that a physician had removed organ tissue from a patient with a rare blood type for research purposes without telling the patient about the intended use and future prospects for profit-making endeavors did not fit neatly into the requirements for conversion, although they did state a claim for breach of the physician's fiduciary responsibility premised on the patient's lack of informed consent to the treatment.[26]

The framework for a remedy lies in the concepts of trade secrets and prima facie tort. The U.S. Court of Appeals for the Second Circuit has declared:

> To succeed on a claim for the misappropriation of trade secrets under New York law, a party must demonstrate: (1) that it possessed a trade secret, and (2) that the defendants used that trade secret in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means. . . .
>
> "[A] trade secret is 'any formula, pattern, device or compilation of information which is used in one's business, and which gives [the owner] an opportunity to obtain an advantage over competitors who do not know or use it.'" In determining whether information constitutes a trade secret, New York courts have considered the following factors:
>
> (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[27]

DNA analysis is a compilation of information that undeniably gives the owner an opportunity to obtain an advantage over competitors who do not know or use it. If insurance companies, health care providers and purveyors of goods and services intend to rely on this information to determine whether to accept customers and how to market their products, the information is priceless. It cannot be duplicated or acquired without cooperation or compulsion. Perhaps most important, the owner must maintain the secrecy of the information in order to emphasize the privacy interest in it. In sum, the results of DNA analysis arguably qualify for trade secrets protection under the traditional theory.

The desire to keep private information private arises from something more than the avoidance of commercial exploitation. The interest is personal and as a result, a

---

25. N.Y. CIV. RIGHTS LAW §§ 50 through 52.

26. Moore v. Regents of Univ. of California, 793 P.2d 479, 487-96 (Cal. 1990).

27. North Atlantic Instruments Inc. v. Haber, 188 F.3d 38, 43-44 (2d Cir. 1999), *quoting* Ashland Management Inc. v. Jamien, 624 N.E.2d 1007, 1013 (1993) (citations omitted). In order to establish federal jurisdiction, the parties would have to satisfy the diversity of citizenship requirements, or the claim will have to qualify for supplemental or pendent jurisdiction. *See* Kirschner v. Klemons, 225 F.3d 227, 239 (2d Cir. 2000).

court may be understandably reluctant to analogize the wrongful disclosure of personal information to a tort that protects interests in business activity. To separate and emphasize the personal nature of the interest protected, the claim may require proof of an additional element or elements.

Recovery for prima facie tort requires proof of "(1) intentional infliction of harm, (2) causing special damages, (3) without excuse or justification, (4) by an act or series of acts that would otherwise be lawful."[28] Its distinguishing feature is that malevolence is the sole motive for the defendant's otherwise lawful act.[29] Comment to Section 870 of the Restatement (Second) of Torts refers to New York's enumeration of the elements as an effort to set forth the requirements with more rigidity. The Restatement employs language intended as a general principle rather than setting forth specific rules:

> One who intentionally causes injury to another is subject to liability to the other for that injury, if his conduct is generally culpable and not justifiable under the circumstances. This liability may be imposed although the actor's conduct does not come within a traditional category of tort liability.

New York's concept of "special damages" may be narrower than in other jurisdictions,[30] although the requirements for special damages may vary with the context.[31]

The combination of elements of trade secrets and prima facie tort results in a cause of action suited to protecting an individual's interest in maintaining the privacy of DNA test results. To recover, plaintiffs would be required to show that the secrecy or confidentiality of their DNA had been maintained. For that reason, the careless deposit of DNA, or substances which contain it, would provide a court with less incentive to protect the privacy interest in nondisclosure.[32] The privacy interest, however, should inhere in the circumstances. A plaintiff should not be required to engage in a ceremony or provide a document to establish that DNA voluntarily given is to be used only for the purpose that has been revealed or agreed on.

Inclusion of the elements of the intentional infliction of harm and special damages reduces the likelihood that this cause of action could be used to seek redress for de minimis or inconsequential revelations.[33] Traditionally, courts have subjected intentional conduct to judicial scrutiny and should be open to the concept of compensating a plaintiff who can demonstrate loss, economic or personal, as a result of the disclosure of private DNA information.

---

28. Curiano v. Suozzi, 469 N.E.2d 1324, 1327 (N.Y. 1984), *aff'g* 477 N.Y.S.2d 13 (App.Div. 1st Dep't 1984). If the means are illegal and corrupt the claim is referred to as "intentional tort." Chen v. United States, 854 F.2d 622, 628 (2d Cir. 1988) (N.Y. law).

29. Burns Jackson Miller Summit & Spitzer v. Lindner, 451 N.E.2d 459 (N.Y. 1983), *aff'g* 452 N.Y.S.2d 80 (App.Div. 2d Dep't 1982).

30. Wahlstrom v. Metro-North Commuter R.R. Co., 89 F.Supp.2d 506, 532 (S.D. N.Y. 2000) (special damages must be pleaded fully and accurately so as to relate causally actual losses to allegedly tortious act or acts.

31. *See* Tomai-Minogue v. State Farm Mut. Auto Ins. Co., 770 F.2d 1228, 1237 (4th Cir. 1985) (in malicious prosecution action, special damages entail some arrest of person, seizure of property, or other injury not ordinarily result in all civil actions) (Mayland and Virginia law); Moore v. Boating Industry Ass'ns, 754 F.2d 698, 716 (7th Cir. 1985) (Illinois law); Patten Corp. v. Canadian Lakes Dev. Corp., 788 F.Supp. 975, 979 (W.D. Mich. 1991) (special damages are those that actually but not necessarily result from alleged injury) (Michigan law); In re Hawaii Fed. Asbestos Cases, 734 F.Supp. 1563, 1567 (D. Hawaii 1990) (special damages compensate for specific out-of-pocket financial expenses and losses) (personal injury; Hawaii law); RESTATEMENT (SECOND) OF TORTS § 904 (1979).

32. *See* Lavalle v. State of New York, 696 N.Y.S.2d 670, 671 (Sup.Ct. Duchess County 1999).

33. *See* Webb v. Goldstein, 117 F.Supp.2d 289, 298 (E.D. N.Y. 2000); D'Andrea v. Rafla-Demetrious, 972 F.Supp. 154, 157 (E.D. N.Y. 1997), *aff'd*, 146 F.3d 64 (2d Cir. 1998) (per curiam).

The Privacy Project

Protection of Personal Data: The United Kingdom Perspective

The U.K.'s new Data Protection Act sets up a comprehensive and detailed regime to which multinationals must conform for the transfer of personal data

By Laurel J. Harbour, Ian D. MacDonald and Eleni Gill

THE EXPLOSION of information power has become a fundamental feature of business worldwide. The operational and commercial success of many organisations depends on their ability to obtain, process and store vast quantities of information about employees, customers and the general public. The same technological progress that has made this possible has, however, brought with it a growing concern on the part of European law makers that its use might weaken or undermine individual human rights, particularly the right to privacy.

The Data Protection Act 1998 (DPA), which came into effect on March 1, 2000, is the latest piece of United Kingdom legislation to regulate the use of personal data.[1] The DPA implements the Directive 95/46/EC 24 October 1995 of the European Parliament and the Council of the European Union on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.[2] The European data protection regime is an attempt to balance the interests of the freedom of the individual, the free movement of information and the freedom to trade.

The U.K. approach to data protection is one of the more liberal in Europe, yet the DPA nonetheless imposes wide-ranging obligations on organisations in relation to their use of personal data. These obligations are far-reaching and, with a few exceptions, apply to all organisations, both public and private, no matter how big or small and regardless of the nature of their operations.

The provisions of the DPA are implemented and enforced by the Information Commission, an independent supervisory

IADC member Laurel J. Harbour is co-managing partner in the London office of Shook, Hardy & Bacon, where she concentrates in commercial litigation, in particular product liability claims against pharmaceutical companies and other manufacturers. She is a graduate of the University of Iowa (B.A. 1969, M.A. 1971, J.D. 1974).

Ian D. MacDonald, formerly a partner in the Canadian law firm Davies Ward Philips & Vineburg, is also a co-managing partner in the London office of Shook, Hardy & Bacon and concentrates in commercial transactions relating to intellectual property. He has a B.A. (1983) from Simon Fraser University in Vancouver, and M.A. (1987) from the University of North Carolina, and an LL.B. from Dalhousie University in Nova Scotia.

An English solicitor, Eleni Gill also is located at Shook, Hardy & Bacon, London. She concentrates in product liability litigation, employment law and data protection issues. She was educated at Manchester Metropolitan University (LPC 1994) and the University of Sheffield (LL.B. 1993).

1. 1998 c. 29. Available at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf. Written answers with respect to the DPA from 10 June 1998 are available at http://www.publications.parliament.uk/cgi-bin/lds98/text/80616w02.htm#80616w02_wqn1

2. 1995 O.J. (L 281) 31-50. Available at http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25

body appointed by the Crown. Richard Thomas has been appointed Information Commissioner effective 1 October 2002, to succeed Elizabeth France, the first commissioner. The DPA gives the commissioner investigative powers, including the power to obtain search warrants and to take action against organisations in breach of the statutory regulations. The commissioner's office has traditionally viewed itself as more of an educator than a regulator and pursued enforcement procedures only in cases of flagrant breach. In 2002, however, it launched a high-profile advertising campaign informing individuals of their rights under the DPA, and it is currently reviewing its enforcement procedures.

This article summarizes the key provisions of the U.K. data protection regime, including the central statutory definitions, the main duties imposed on organisations that process personal data ("data controllers"), the rights of individuals about whom personal information is being processed ("data subjects"), and the regulation of transborder data flows.

SCOPE OF THE DPA

The DPA regulates the "processing" of "personal data." "Data" is defined as computerized information as well as personal data in manual files, provided the data are "recorded as part of a relevant filing system." A "relevant filing system" is defined as "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible." This would include, for example, paper files or card indexes that permit ready access to specific information relating to particular individuals.

Personal data are any "data which relate to a living individual who can be identified—(a) from those data, or (b) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller." This concept is interpreted broadly. It covers information concerning an individual in both a personal and business capacity (as in the case of a sole trader) and also includes any expression of opinion or intention about the data subject, which is clearly relevant in the personnel context.

Contact names and addresses, e-mail addresses and clinical data, for example, are all considered personal data. An additional category of "sensitive" personal data under the DPA includes, among other things, data relating to the racial or ethnic origin, political opinions, religious beliefs and physical or mental health of an individual. More stringent regulations apply to the processing of personal data categorized as "sensitive."

The DPA applies to personal data that are "processed." This is an extremely broad provision, so broad, in fact, that the commissioner in a legal guidance has stated that "it is difficult to envisage any action involving data which does not amount to processing within this definition." The statute defines "processing" as

> obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making it available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.

Under this definition, processing includes virtually any activity performed on data from holding personal data, to pulling up information on a computer screen, to storing personal data on a computer hard drive.

DPA DATA PROTECTION PRINCIPLES

A. The Principles

The DPA imposes an obligation on data controllers to comply with statutory prin-

ciples of good information handling, known as the Data Protection Principles (DPP), of which there are eight:

- First, personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 of the DPA is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 also is met.
- Second, personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Third, personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Fourth, personal data shall be accurate and, where necessary, kept up to date.
- Fifth, personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Sixth, personal data shall be processed in accordance with the rights of data subjects under the DPA.
- Seventh, appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Eighth, personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data.

B. Interpretation of the Principles

These principles, which are the backbone of the data protection legislation, impose significant obligations on data controllers in the way they obtain, use, store and transfer personal data. Not least is the requirement for data controllers in the first principle to ensure that data is processed "fairly and lawfully."

Paragraphs 1 to 4 of Part II of Schedule 1 of the DPA contain interpretive provisions relating to fairness, which are referred to as the "fair processing requirements."

Compliance with the fair processing requirements in itself will not ensure that processing is fair; it is to be seen as a minimum standard of compliance. The fair processing requirements include consideration of the method by which the data are obtained, including whether any person from whom they are obtained is misled about the purpose for which they are to be processed. Furthermore and subject to certain exceptions, data are not to be regarded as processed fairly unless the individual about whom personal data are to be processed is told the identity of the data controller, the purpose for which the data are to be processed and any other information which is necessary for processing to be fair.

There is no statutory definition of lawful processing, but the commissioner's guidance considers that it includes compliance with all relevant rules of law, both statutory and common law, that relate to the purpose and ways in which the data controller processes personal data. This would include compliance with the DPA itself and compliance with common law rules—for example, those relating to confidentiality.

Furthermore, the first principle states that personal data may not be processed unless at least one of a list of statutory conditions is satisfied. These are known as the Schedule 2 conditions and include that the individual has given consent to the processing or that the processing is necessary for the purposes of the legitimate interests pursued by the data controller, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject . In the case of sensitive personal data, in addition to compliance with one of the conditions of Schedule 2, the data controller must also comply with at least one of the conditions set out in Schedule 3, which include a requirement for explicit consent from the

data subject or a requirement that processing is necessary for one or more permissible purposes, such as performance of employment law obligations or the exercise or defence of legal rights.

The second principle requires, furthermore, that personal data may be processed only for lawful and specified purposes, which are notifiable to the commissioner or directly to the data subject. Personal data may not be processed in a way that is inconsistent with those purposes.

Organisations should ensure that personal data are adequate, relevant and not excessive given the purposes for which they are processed. In other words, under the third principle organisations should identify the least amount of information required to fulfill that purpose properly.

The fourth and fifth principles require that personal data must be kept accurate and up to date and should not be kept longer than necessary for the purposes for which they are being processed. In addition, under the seventh principle, appropriate steps should be taken to guard against unlawful or unauthorized processing of personal data or against accidental loss or destruction.

Measures such as controlling access to personal data by the provision of secure areas and passwords, staff selection and training procedures and policies for detecting and dealing with breaches of security may be appropriate, depending on the circumstances.

NOTIFICATION TO COMMISSIONER

A significant aspect of the U.K. data protection regime is the requirement that data controllers inform the commissioner that they are processing personal data, a procedure referred to as "notification." The processing of personal data without notification is a criminal offence, subject to certain exceptions, which include processing for the purpose of staff administration, advertising, marketing, public relations and accounts and records. For the most part, there is no requirement to notify the commissioner about manual processing, again subject to some exceptions, although the remaining provisions of the DPA still apply, including the data protection principles.

The notification procedure requires the data controller to provide certain information to the commissioner annually, together with a fee, which was set at £35 as of the fall of 2002. This information, which can be supplied by post, telephone or Internet, is entered onto a public register, named the Data Protection Register. The data controller must specify the (a) "registrable particulars" and (b) a general description of the measures to be taken to ensure compliance with the Seventh Principle, which relates to security measures to protect data.

The "registrable particulars" include (a) the data controller's name and address, (b) a description of the personal data being or to be processed and the category of data subjects to which they relate, (c) a description of the purpose of processing, (d) a description of any intended recipients of the data, and (e) a list of the countries outside the European Economic Area that will or might receive the data from the data controller. Other than the description of security measures taken to protect data, all the information provided by the data controller appears on the public register.

TRANSFERS OUTSIDE THE E.E.A.

A. General

A noteworthy aspect of the U.K data protection regime, particularly for organisations with global interests, is the prohibition on transfers of personal data to countries outside the European Economic Area that do not ensure an "adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data," to quote the eighth principle.[3]

3. The European Economic Area consists of the 15 member states of the European Union, plus Iceland, Liechtenstein and Norway.

B. Exceptions

There are certain important statutory exceptions to the prohibition on the transfer of personal data, which are set out in Schedule 4 of the DPA:

- The data subject has given consent to the transfer.
- The transfer is necessary for the performance of a contract between the data subject and the data controller or for the taking of steps at the request of data subjects with a view to their entering into a contract with the data controller.
- The transfer is necessary (a) for the conclusion of a contract between the data controller and a person other than the data subject which (i) is entered into at the request of the data subject or (ii) is in the interests of the data subject, or (b) for the performance of such a contract.
- The transfer is necessary for reasons of substantial public interest.
- The transfer (a) is necessary for the purpose of or in connection with any legal proceedings, including prospective legal proceedings; (b) is necessary for the purpose of obtaining legal advice; or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- The transfer is necessary in order to protect the vital interests of the data subject.
- The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.
- The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.
- The transfer is made on terms of a kind approved by the commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.
- The transfer has been authorised by the commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

In addition to the statutory exceptions, the European Commission has determined that transfers to certain countries, including Hungary, Switzerland and Canada (for certain transfers), are "safe" because their domestic law ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The effect of the European Commission's formal findings is that personal data may be freely transferred to these countries.

It is significant that the United States, with its mixture of self-regulation and sector-specific rules, is not considered by the European Union to be a country that provides an adequate level of protection for personal data. As a result, and after considerable discussion, the U.S. Department of Commerce and the European Commission negotiated a scheme referred to as the "safe harbour" agreement.

This is a voluntary scheme, administered by the U.S. Department of Commerce requiring companies to declare publicly their membership in the safe harbour and abide by rules similar to those in force in Europe governing the use of personal data. The rules include notification to individuals as to the purpose and use for which data is collected, adequate security measures and restrictions on data transfers to third parties. U.K. data controllers may make a presumption of adequacy for data transferred to U.S. organisations that have signed up to the terms of the safe harbour agreement.

C. Assessing "Adequacy"

It is the responsibility of the data controller to determine whether there is an adequate level of protection in the non-E.E.A. country to which the data is being transferred. In practical terms, an adequacy assessment must be undertaken where the transfer is not covered by a Schedule 4 exemption or where the third country to which the data is being transferred has not been designated as "adequate" by the Euro-

pean Commission. In these circumstances, data controllers should consider whether the third country has data protection provisions similar to those afforded to individuals by the E.U. directive.

The DPA suggests various factors that data controllers should consider in assessing adequacy, including the nature of the personal data; the country of final destination of the information; the law, relevant codes of conduct and international obligations of the third country; and security measures taken regarding data in the third country. The commissioner has issued detailed guidance for assessing adequacy, which is available on the commission website.[4]

As an alternative to an adequacy assessment, the data controller in the U.K. may enter into a contract with the recipient of data in the third country requiring adherence to certain principles of data protection. The European Commission recently approved model terms that can be incorporated into such a contract. Data controllers who enter into contracts based on the model clauses can transfer personal data to the other party in a third country without the need to make an assessment of adequacy. The standard contractual clauses provide for compliance by the data importer with "Mandatory Data Protection Principles" concerning, for example, security and confidentiality, rights of access, rectification of data, and restrictions on onward transfers.

RIGHTS OF DATA SUBJECTS

Concern for the individual's right to privacy is evidenced in the provisions of the DPA enabling data subjects to obtain information about the processing of personal data and to prevent certain types of processing from taking place.

On written request and payment of a fee, data controllers must tell individuals whether their personal data are being processed and, if so, give them a description of the data, the purposes for which data are being processed and those to whom the data are or may be disclosed. In addition, the data controller must communicate, in an intelligible form, the information to requesters and any information available to the data controller about the source of those data.

There are some exceptions to the right to access, including an exemption for information subject to legal professional privilege, processing undertaken for the "special purposes" (journalistic, literary or artistic) and the prevention or detection of crime.

Data subjects also have several options open to them to control the activities of organisations that process their personal data. First, they may request the data controller not to process personal data where to do so would result in unwarranted and substantial damage or distress to the data subject or to another. This does not apply where the data subject has consented to the processing or where the processing is necessary for the performance of a contract to which the data subject is a party, for compliance with a non-contractual legal obligation or for the protection of the vital interests of the data subject.

Second, data subjects may prevent processing for the purpose of direct marketing, which includes sending mail to individuals promoting a certain product or service and also targeting an individual's e-mail account.

Third, under Section 14 of the DPA, where a court is satisfied that personal data being processed by the data controller are inaccurate, the court may order rectification, blocking, erasure or destruction of the data.

Fourth, the data controller can be prevented from making decisions about an individual by automated means alone.

Fifth, individuals who believe that they are being directly affected by the processing of personal data may request the com-

---

4. The Eighth Data Protection Principle and Transborder Data Flows, available at http://www.dataprotection.gov.uk. The guidance is stated to be the preliminary view of the Information Commissioner and "reflects the current state of thinking" and that the commissioner's "views have been (and will be) informed by continuing international negotiations and discussions."

missioner to assess the processing to determine whether it adheres to the provisions of the DPA. Such assessments may result in the issuing of an information notice or an enforcement notice.

Data subjects are entitled to claim compensation for any damage suffered as a result of a breach of the DPA by a data controller and also may claim compensation for distress. It is a defence to a claim for compensation for a data controller to show it took reasonable care, given all the circumstances, to comply with the provision in question.

ENFORCEMENT

The Information Commissioner is responsible for enforcing the provisions of the DPA. The commissioner has the power to serve information notices and enforcement notices. A data controller served with an information notice must supply information to the commissioner that is sufficient for a determination whether the processing breaches the DPA. The commissioner may serve an enforcement notice when satisfied that a data controller is contravening the provisions of the DPA. An enforcement notice requires the data controller to take certain specified steps to rectify the breach, including rectifying, blocking, erasing or destroying personal data. Failure to respond appropriately to a notice served by the commissioner is a criminal offence, although a data controller is exempt from complying with an information notice if the required information is subject to legal privilege. It is a defence for the data controller to show that it exercised due diligence to comply with an enforcement notice.

The commissioner also has the power to apply to a circuit judge for a warrant to enter and search premises when there are reasonable grounds for suspecting that the DPA is being violated or an offence committed. With a warrant, the commissioner has wide-ranging powers to enter and search premises for evidence of the offence or contravention; to inspect, examine, operate and test equipment used for processing personal data; and to inspect and seize any documents or other material that may be evidence of an offence or contravention of the DPPs.

PRACTICAL TIPS

The DPA is still a relatively new piece of legislation and it is still unclear how the courts will apply the data protection provisions in practice. The commissioner, however, has issued a useful guidance document with interpretations of the statutory provisions. The commissioner also has provided advice on a range of subjects, including transborder data flows, notification, the Internet and the use of personal data in employer-employee relationships.

Organisations currently based in the U.K., planning to locate a branch there or considering transferring data from the U.K. should ensure that their internal data protection policies and procedures comply with the statutory regime. The following are examples of some issues that an organisation may want to consider:

- Implement a data protection compliance program.
- Appoint a data compliance representative, whose role it is to monitor the processing of personal data to ensure compliance with the DPA.
- Review the organisation's annual notification requirements.
- Implement training programs for all relevant personnel.
- Implement technological and organisational measures to protect personal data from unlawful or unauthorized processing, damage, loss or destruction.
- Obtain the consent of data subjects to processing of personal data.
- Obtain the consent of data subjects to transfers of personal data to countries outside the E.E.A. Otherwise, consider whether the transfer satisfies the commissioner's "good practice approach" to transborder data flows.

The Privacy Project

Protection of Personal Data: The Australian Perspective

New legislation has applied the information privacy principles of 1988 to the private sector through national privacy principles

By Steven Klimt, Narelle Symthe, S. Stuart Clark and Jason Shailer

THE MAIN data protection law in Australia in relation to privacy is the Privacy Act 1988 (Cth). It has been amended by the Privacy Amendment (Private Sector) Act 2000 (Private Sector Act), which came into operation in December 2001 and effectively extends the operation of the 1988 act to the private sector.

The regime introduced by the Private Sector Act has far-reaching consequences for both the business community and consumers in Australia. The stated aim is to reduce obstacles to the development, take-up and use of electronic commerce and other new technologies resulting from concerns about the possible mishandling of personal information by the private sector, while at the same time avoiding excessive red tape and minimising the cost of compliance on business.

The 2000 Act creates a co-regulatory legislative framework through the development of self-regulatory codes of practice by organisations that must achieve certain minimum standards of privacy protection set out in 10 National Privacy Principles (NPPs) in the act. The NPPs are the core of the private sector regime and establish minimum standards in relation to the collection, holding, use, disclosure, management, access, correction and disposal of personal information about natural persons. The NPPs also include special measures with regard to certain types of personal information defined as sensitive. In the absence of a relevant self-regulatory code, the NPPs themselves will apply.

Steven Klimt is a partner in the Sydney office of the Australian national law firm Clayton Utz, where he concentrates his practice in electronic commerce and retail banking. He holds B.A., LL.B. and LL.M. degrees from Sydney University.

Also a partner in the same office, Narelle Symthe has experience in electronic commerce and information technology litigation. She was educated at the University of New South Wales (B.Com. and LL.B.).

IADC member S. Stuart Clark, a member of the IADC Executive Committee, also is a partner in the firm and heads the product liability group. He concentrates in the defense of complex litigation and class actions. He received his B.A. and LL.B. degrees from Macquarie University in Sydney, and is admitted to practice in New South Wales, Victoria, South Australia and the Australian Capital Territory.

A graduate of Sydney University (B.A. and LL.B.), Jason Shailer is an associate at Clayton Utz.

The requirements of the Private Sector Act have affected, directly or indirectly, all businesses in Australia. Organisations subject to regulation under the act have been required to implement changes to transactional documents, internal and external information handling and security procedures, information technology requirements, customer communications and training of staff in order to comply with the new regime. Maintaining compliant information-handling practices is a continuing challenge.

It is important to note that the Private Sector Act does not stand alone. Regula-

tion of information-handling practices in Australia intended to protect individuals' privacy has existed in a number of forms prior to the Private Sector Act, although these existing regimes will not be considered in any detail in this article.

A number of state and territory governments have enacted legislation affecting their governments' dealings with individuals' personal information—for example, the Privacy and Personal Information Act 1998 in New South Wales. Other existing forms of regulation of information-handling practices affecting the private sector include (1) common law obligations of confidentiality; (2) a number of statutory mechanisms affecting specific industry sectors; and (3) voluntary codes of conduct adopted by industry groups—for example, the Insurance Council of Australia, the Australian Direct Marketing Association, and the Australian Bankers Association.

The 1988 Act required federal government agencies to act in accordance with 11 Information Privacy Principles (IPPs), which are broadly similar to the NPPs. The Privacy Act applies these to private sector organizations (1) in relation to the collection, storage, use and security of tax file number information; and (2) in relation to the information-handling practices of credit reporting agencies, credit providers and associated persons.

SCOPE OF PRIVATE SECTOR REGIME

The Private Sector Act introduced a new regime, termed the "the private sector regime," which operates within the existing structure of the 1988 Privacy Act. References in this paper to sections are, unless otherwise stated, references to sections of the Privacy Act 1988, as amended by the Private Sector Act.

The 2000 act extends regulation of handling of all forms of personal information across the private sector, and it introduces new provisions and modifies a number of existing provisions, while leaving the pre-existing obligations on private sector organisations regarding tax file number information and credit reporting practices in place.

A. What Is Regulated?

1. Personal Information

The handling of "personal information" is regulated. Personal information is defined in Section 6 as:

> Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or an opinion.

By way of example, this is not personal information, if this information alone is collected by an organisation: "male, 180 cm tall, blue eyes." The identity of the individual is not apparent, nor can it reasonably be ascertained from the information, even if, when combined with other information, the identity of an individual could be ascertained. However, this is personal information: "[name] male, 180cm tall, blue eyes." From this information the identity of an individual could reasonably be ascertained.

2. Sensitive Information

The private sector regime imposes additional requirements on an organisation with respect to "sensitive information." Sensitive information is defined in Section 6(1) as:

> Information or an opinion about an individual's:
> - racial or ethnic origin; or
> - political opinions; or
> - membership of a political association; or
> - religious beliefs or affiliations; or
> - philosophical beliefs; or
> - membership of a professional or trade association; or
> - membership of a trade union; or
> - sexual preferences or practices; or
> - criminal record;
>
> that is also personal information; or
> - health information about an individual.

Essentially, an organisation is not permitted to collect sensitive information except (1) with the consent of the individual; (2) where required by law; (3) in limited circumstances, associated with a non-profit organisation's[1] dealings with its members (or individuals in regular contact with that organisation in the course of its activities); or (4) where collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

In limited circumstances, sensitive information that is health information may be collected if it is necessary to provide a health service to an individual or for research purposes, where it is not possible to use de-identified information.

B. Commencement and Application

The Private Sector Act commenced on 21 December 2001. However, special provision was made for certain small businesses, which will benefit from a delayed application period of up to 12 months after 21 December 2001.

The NPPs regulating collection, use and disclosure of personal information apply to personal information collected only on or after 21 December 2001. Personal information collected before that date may be used or disclosed by an organisation without reference to the requirements of the second NPP, which regulates use and disclosure of personal information. However, in many cases it is not practical for organisations to have separate procedures for use and disclosure of personal information they hold, depending on whether that information was collected before or after the commencement of the private sector regime.

In any event, organisations have obligations under the NPPs with respect to the accuracy and completeness, security and disposal, policies for management, access and correction,[2] and transborder movement of personal information in their possession, even if that information was collected before commencement of the private sector regime.

1. Who Is Affected?

The private sector regime applies to the acts and practices of "organizations," a term that includes bodies corporate, unincorporated associations, partnerships, trusts and individuals. Section 6C. However, some entities are excluded from the definition of organization—for example, small business operators. Certain acts and practices—for example, employee records—are exempt. These exclusions and exemptions are dealt with below.

2. Who and What Are Excluded?

a. Private Affairs

Individuals may be subject to regulation under the act as an "organisation" in relation to their business activities. Acts and practices of individuals which are organisations other than in the course of a business carried on by the individual are exempt. Section 7B(1). Moreover, Section 16E expressly excludes the collection, holding, use or disclosure or transfer of personal information by an individual, or personal information held by an individual for the purposes of, or in connection with, his or her personal, family or household affairs.

The term "personal, family or household affairs" is not defined. Existing case law defining "in the course of a business" may provide a guide to determining the circumstances that fall within this exemption.

b. Employee Records

The act provides an exemption for the collection, use or disclosure of information contained in employee records in the context of employment relationships. Section 7B(3) states that an act done, or practice engaged in, by an organisation that is or was an employer of an individual, is exempt if the act or practice is directly related to (1) a current or former employment rela-

1. Defined to mean a non-profit organization that has only racial, ethnic, political, religious, philosophical, trade or trade union aims.

2. Except to extent that compliance places an unreasonable administrative burden on the organisation or causes the organisation unreasonable expense.

tionship between the employer and the individual; and (2) an employee record held by the organisation and relating to the individual.

Employee records are defined broadly to include, for example, a record containing information about the engagement, training, disciplining or resignation of an employee; the terms and conditions of employment of an employee; or an employee's performance or conduct. Section 6. The rationale for the exemption is that handling of employee records is an issue best dealt with under workplace relations legislation.[3]

The requirement that the act or practice be related to a current or former employment relationship and an employee record held by the organisation and relating to the individual means that once information contained on an employment record is disclosed by the current or former employer, the use and disclosure by the persons to whom it is disclosed is not be exempted, unless they too are an employer of the individual and their use or disclosure is directly related to an employee record held by them.

By way of example, if an employer discloses records containing personal information of an employee to the employee's insurer for the purposes of workers' compensation, the insurance company will not enjoy the exemption provided by Section 7B(3) and would be subject to the NPPs in collecting, using and disclosing that information.[4]

The further requirement that the act or practice be directly related to the employment relationship and an employee record held by the organisation prevents an employer organisation from selling personal information about an employee to a third party, which would be considered not "directly related" to the current or former employment relationship.

A number of issues arise from the employee records exemption, including the following:

- The exemption attaches only to circumstances where a current or former employment relationship exists. Acts and practices with respect to personal information about prospective employees or job candidates do not fall within the exemption unless those individuals happen also to have been former employees. Organisations may need to use forms of disclosure or consent for any personal information collected from job candidates. If the information, once collected, is held in an employee record about that individual and an employment relationship is established, then, if the other requirements of the exemption are satisfied, use and disclosure of that information may fall within the exemption.
- "Record" is defined to include a database, however kept. The breadth of the definition of employee record (a record of personal information relating to the employment of the employee) may mean that, for example, a daily back up tape or disk holding copies of e-mails is an "employee record" and thus subject to the exemption.

The federal government has foreshadowed that a review of existing state and territory laws affecting employee records will be carried out by the Attorney General's Department and the Department of Employment, Work Place Relations and Small Business, in consultation with state and territory governments, the Privacy Commissioner and other key stakeholders. The government has stated that this review will be completed in time to assist the Privacy Commissioner to conduct a more general review of the act after 22 December 2003, two years after it commenced operation.

c. Related Bodies Corporate

Section 13B provides that each of the following acts or practices of an organisation that is a body corporate is not an "interference with the privacy" of an individual: (1) the collection of personal

3. Revised Explanatory Memorandum circulated by Attorney General ("Revised EM"), Item 109, hereinafter Revised EM.

4. Set out in "Employee Records," a fact sheet released by the Attorney General, 22 December 2000.

information (other than sensitive information) about the individual by the body corporate from a related body corporate; or (2) the disclosure of personal information (other than sensitive information) about the individual by the body corporate to a related body corporate.

Related body corporate is defined by reference to Section 50 of the Corporations Act, which is Commonwealth of Australia legislation. The exemption with respect to related bodies corporate extends to the collection of information from and disclosure of personal information only to related bodies corporate. The use and disclosure by the organisation that collects personal information from a related body corporate remains subject to the requirements of NPP 2 and 10. The related body corporate exemption does not apply to acts or practices of contracted service providers for the commonwealth that may be interferences with privacy.

The related body corporate exemption does not provide organisations with a means of avoiding the requirements of NPP 1 with respect to collection of personal information. For example, if an exempt entity such as a media organisation acting in the course of journalism collects personal information and then discloses it to a related body corporate subject to the act, the exemption does not allow the body corporate collecting the personal information from the exempt entity to avoid its obligations under the NPPs. This is because the related body corporate exception does not apply to the act of collection by body corporate B from body corporate A, even if A and B are related bodies corporate, if: (1) A is not an organisation as defined in the act (for example, if A is a registered political party); or (2) A is an organisation but the disclosure of the personal information by A will be an exempt act or practice (for example, media organisation acting in the cause of journalism); (3) or A is compelled to make the disclosure to B under an applicable law of a foreign country.

Where personal information is collected by body corporate B from body corporate A (A being a related body corporate of B) the primary purpose of collection of body corporate A will be taken to be the primary purpose of collection of B.[5] In other words "the primary purpose is transferred with the personal information when it is shared around the group of related bodies corporate."[6]

d. Changes to Partnerships

Section 13C ensures that where a partnership which is an organisation is dissolved and a new partnership is immediately established to carry on the same business, with at least one partner who was also a partner of the dissolved partnership, the passage of personal information about an individual from the old partnership to the new partnership does not constitute an interference with the privacy of the individual where it is necessary for the new partnership to hold the information immediately after its formation.

This provision avoids the obvious difficulties that might arise in the ordinary course of changes to the composition of partnerships.

e. Small Business Operators

(i) Scope of the Exclusion

The act excludes small business operators from the definition of organisation. This means they are effectively exempt from the operation of the act. The definition of small business operator is not straightforward and contains several complex exemptions.

Section 6B of the act defines both a "small business" and a "small business operator." A small business is defined with respect to an annual turnover figure. A small business operator is then defined as an entity that carries on one or more small businesses and does not carry on a business that is not a small business.

---

5. "Primary purpose" is not defined in the act, but it appears that it will be the "main purpose for which the information was originally collected." Revised EM, Item 141.
6. Revised EM, Item 142.

(ii) Turnover Calculations

Section 6D defines a small business by reference to a "test time" in a financial year and the annual turnover of the business for the previous financial year, which must be A$3 million or less. Broadly, the annual turnover is the sum of the business's income and proceeds of sales.

If the business was not carried on in the previous financial year, it is still considered a small business if its annual turnover for the current year is A$3 million or less. In order to determine the annual turnover for a current year, Section 6DA(2) of the act provides a formula that takes the business's actual turnover for that part of the year already passed and extrapolates it over a full year.

An entity is not considered a small business operator if any business it conducts has an annual turnover exceeding A$3 million in any financial year ending after the commencement of the act.

(iii) Small Businesses Dealing in Health Information

Regardless of whether its annual turnover is less than the threshold, Paragraph 6D(4)(b) of the act provides that an entity is not a small business operator if it provides a health services and holds any health information, unless (1) the health information is only held in an employee record; or (2) the health information is held only otherwise than in the course of a business (and, where the entity is an individual, the health information is held only for personal, family or household affairs).

(iv) Small Business Trading in Personal Information

Paragraph 6D(4)(c) and (d) provide that an entity is not a small business operator if it discloses personal information about an individual to someone else for a benefit or provides a benefit to someone else to collect personal information about another individual, unless (1) the information is disclosed or collected with the consent of the other individual; (2) the information is disclosed or collected as required or authorised by or under legislation; or (3) the information is disclosed or collected otherwise than in the course of a business (and, where the entity is an individual, the information is disclosed or collected only for personal, family or household affairs).

(v) Small Businesses as Service Providers for Commonwealth Contract

An entity is not a small business operator if it is a contracted service provider for a Commonwealth of Australia contract. This applies whether or not the entity itself is a party to a contract with the Commonwealth. This means that sub-contractors to Commonwealth contractors are not small business operators.

However, to the extent that an entity would otherwise be a small business operator, Section 7B(2) ensures that the activities of that entity not carried out in the performance of their obligations under the Commonwealth contract are exempt from the act.

(vi) Small Business Operators Can Opt In

Under Section 6EA, small business operators can elect to be treated as though they were an organisation covered by the act. The choice is required to be made in writing to the Privacy Commissioner, as a result of which the Privacy Commissioner is required to enter details about the small business operator into a register. The small business operator is then treated as an organisation covered by the act for as long as its choice is registered. The choice can be revoked by notice to the Privacy Commissioner in writing, in which case the Privacy Commissioner must remove the small business operator from the register.

If a small business chooses to opt in and then later revokes its choice, it follows that the acts and practices that it engaged in while its choice was registered may still be investigated and dealt with by the Privacy Commissioner. This ensures that the Privacy Commissioner's jurisdiction to inves-

tigate complaints is not defeated by a business reasserting exempt status after the act or practice complained of occurred.

(vii) Delayed Application of NPPs

The act provides for delayed application of the NPPs to entities that satisfy the requirements to be to small businesses but are not small business operators. An example would be an entity that carries on a small business involving the disclosure of personal information about individuals to other persons for reward, where the disclosure is not made with the individuals' consents or as required or authorised by legislation.

The effect of the delayed application period for these small businesses is that:

- Until the delayed application period has ended, collection of personal information will not be subject to NPPs 1, 3 and 10.
- NPPs 3, 4, 5, 7 and 9 will apply only to the use and disclosure of personal information taking place after the delayed application period has ended.
- Once the delayed application period has ended, NPPs 3, 4, 5, 7 and 9 will apply to personal information held by the organization, whether it was collected before, during or after that period.
- NPP 2 will only affect the use and disclosure of information collected after the delayed application period ends. NPP 6, which sets out obligations with respect to access and correction, apply only to personal information collected after the delayed application period ends.

An organisation's obligation wherever lawful and practicable to provide individuals with the opportunity of not identifying themselves when entering a transaction under NPP 8 apply only to transactions entered into after the delayed application period ends.

(viii) Power to Prescribe Certain Small Businesses

Section 6E(4) allows the Attorney General, if it is in the public interest and after consultation with the Privacy Commissioner, to prescribe small business operators as organisations for the purposes of the act. When consulting the Privacy Commissioner, the Attorney General must consider the views of other interested people, such as the Minister for Small Business and the Privacy Advisory Committee, to which a small business representative has been appointed.

(ix) Related body corporate exemption

Section 6D(9) makes it clear that a body corporate is not a small business operator if it is related to a body corporate that carries on a business that is not a small business. In other words, the related body corporate exception, which is described above, does not provide a means by which a large organisation may circumvent the requirements of the NPPs by collecting personal information through a related body corporate that is a small business operator.

f. Media Organisations Acting in Course of Journalism

Section 7B(4) provides that acts or practices engaged in by a media organisation in the course of journalism are exempt from the act. The policy imperatives behind this exemption are reasonably clear—there is a public interest in the "free flow of information through the media."[7]

Media organisations are defined in Section 6 as organisations whose activities consist of or include collection, preparation for dissemination or dissemination to the public of material having the character of news, current affairs, information or a documentary or commentary or opinion on or analysis of news, current affairs, information or a documentary. Journalism itself is not defined.

The definition of media organisation is relatively broad—the activities of the or-

7. "Privacy and the Media," a fact sheet released by the Attorney General, 22 December 2000.

ganisation need include only those described above. The question arises whether the exemption might be abused. However, Section 7B(4)(b) provides that for the act or practice to be exempt, the media organisation at the time must have been "publicly committed to observe standards that . . . deal with privacy in the context of activities of a media organisation (whether or not the standards also deal with other matters)," and which have been published in writing by the organisation or a person or body representing a class of media organisations. This provides a safeguard against organisations seeking to exploit the exemption.

The acts or practices of employees of a media organisation in the course of their employment are treated as acts and practices of the organization; the employees are not themselves treated as "organisations." This provision, Section 8, is of general application to organisations under the act.

g. Registered Political Parties and Political Representatives

A registered political party is expressly excluded from the definition of "organisation." The act also provides a limited exemption for certain acts and practices of (1) members of Parliament; (2) local government councillors; (3) the contractors of members of Parliament, local government councillors and political parties; (4) the subcontractors of these contractors; and (5) volunteers working for political parties; when the acts and practices are carried out in connection with an election under an electoral law, a state, territory or commonwealth referendum or in connection with participation of the member, counsellor or political party in another aspect of the political process.

h. Commonwealth Government Agencies

Most Commonwealth Government agencies are regulated by the IPPs in Part III, Division 1, of the 1988 Act. Although they are substantially similar, there are some slight differences between the IPPs and the NPPs, mainly in relation to the use and disclosure of personal information.

Section 6A(2) provides that an act or practice of an organisation that is a contracted service provider under a Commonwealth contract (a contract under which services are provided to a Commonwealth agency) and which is done for the purposes of meeting an obligation under that contract does not breach the NPPs, provided that the act or practice is authorised by a provision of the contract inconsistent with the particular NPP. Section 6B(2) applies similarly in relation to the requirements of an approved privacy code.

What this essentially means is that government contractors can engage in acts and practices that are inconsistent with the NPPs or an approved code, provided that those acts or practices are required to fulfil their obligations under their contract with the government. Section 95B provides that government agencies entering into a commonwealth contract must ensure that they take contractual measures to ensure that a contract service provider does not do an act, or engage in a practice, that would be a breach of an IPP if it had been done by the agency. The agency also must ensure that the contract prevents any subcontracts from authorising a breach of the IPPs.

Individuals cannot enforce the contractual obligations placed on government contractors to comply with the IPPs, as they will not be a party to the contract. However, Section 13A(1)(c) of the act extends the definition of an "interference with the privacy of an individual" to cover situations where contracted service providers breach any contractual obligations that impinge on the NPPs.

The result of this is that there is an interference with the privacy of an individual where (1) an organisation engages in an act or practice that relates to the personal information of an individual, (2) the organisation is a contracted service provider for a commonwealth contract, (3) because a provision of that contract is inconsistent with the NPPs or an approved privacy code a particular act or practice is, under Section 6A(2), not a breach of the NPPs or the

code, (4) the act or practice is done in a manner that is contrary to, or inconsistent with, the relevant provision of the commonwealth contract,

Section 16F expressly prohibits a contracted service provider for the Commonwealth from using or disclosing personal information collected for the purpose of meeting obligations under a commonwealth contract for direct marketing when that use or disclosure is necessary to meet, directly or indirectly, obligations under the commonwealth contract. The provision expressly overrides NPP 2.1, which provides an exception to the restrictions on the use and disclosure of personal information for secondary purposes where that secondary purpose is direct marketing.

An individual may make a complaint to the Privacy Commissioner in respect of the above matters under Section 36(1C). Additionally, Section 40A requires an adjudicator of an approved privacy code to refer a code complaint to the Privacy Commissioner if the complaint is about an act or practice of a contracted service provider under a commonwealth contract.

As noted above, contracted service providers that are otherwise small business operators are in the same position as a small business operator for the purposes of the act in respect of any of their activities that do not relate to the commonwealth contract.

i. State and Territory Government Agencies

State and territory government agencies and organisations are not regulated by the act, so in the absence of specific state or territory legislation, they are not required to comply with the NPPs or similar privacy principles. A number of states and territories have privacy legislation that imposes protection principles similar to the NPPs on their respective agencies and instrumentalities. For example, in New South Wales, the Privacy Personal Information Act 1998 (NSW), and in Victoria, the Information Privacy Act (Vic) 2000.

NEW RULES FOR PRIVATE SECTOR

A. NPPs

The standards by which acts and practices of private sector organisations affecting personal information handling are judged for the purposes of the act are found in the NPPs. Other provisions essentially provide a means of giving effect to and enforcing those standards. Following is a summary of the NPPs.

1. Principle 1—Collection

An organisation is prohibited from collecting personal information unless the information is necessary for one or more of its functions. An organisation must not collect personal information other than in a lawful, fair and not unreasonably obtrusive way and must disclose certain information at or before the time it collects personal information, including its identity and the purpose for which the information is collected. Subject to some exceptions, organisations should collect personal information about individuals only from the individuals themselves.

2. Principle 2—Use and Disclosure

The essence of this principle is that, generally speaking, an organisation is prohibited from using or disclosing information for a purpose other than the primary purpose for which the information was collected. There are a number of exceptions, including (1) where the individual has consented; (2) where the secondary purpose for which the personal information will be used is related (or, in the case of sensitive information, directly related) to the primary purpose and a person would reasonably expect the personal information to be used or disclosed in that way; (3) the use of "non-sensitive" personal information in direct marketing, subject to conditions, which include a right for the individual to opt out of further direct marketing after the first contact).

3. Principle 3—Data Quality

An organisation must take reasonable steps to ensure the accuracy and currency of personal information in its possession.

4. Principle 4—Data Security

An organisation must take reasonable steps to secure the personal information in its possession from misuse and loss and from unauthorised access, modification or disclosure, and must destroy or de-identify the information if it is no longer needed.

5. Principle 5—Openness

An organisation must have documented and accessible policies with regard to the management of personal information and must also inform a person, upon request, of the sort of personal information that it holds, the purposes for which it is held and how the information is collected, held, used and disclosed.

6. Principle 6—Access and Correction

An organisation must provide individuals with access to personal information held about the individual, other than in exceptional circumstances, and incorporate processes for the correction of the information on the request of the individual, or if there is some disagreement as to the correction, allow a statement to be associated with the information noting that the individual desires a correction.

7. Principle 7—Identifiers

In general terms, there is a prohibition on the use by organisations for their own purposes of identifiers assigned by government agencies (such as tax file numbers, and Medicare numbers).

8. Principle 8—Anonymity

Unless unlawful or impractical, individuals must be given the option of not identifying themselves when transacting with an organisation.

9. Principle 9—Transborder Data Flows

Essentially, this principle applies to transfers of information outside Australia, the intention being that effective privacy protection must be ensured in respect of such transfers, subject to limited exceptions, including where the individual has consented or where there is evidence of reasonable steps undertaken by the organisation to ensure that any information transferred will not be held, used or disclosed inconsistently with the NPPs.

10. Principle 10—Sensitive Information

Other than in exceptional circumstances, an organisation is not permitted to collect sensitive information. Exceptional circumstances include where the individual has consented or where the collection is necessary for the protection of an individual who is physically incapable of giving or communicating consent. There are a number of exceptions in relation to health services provision and public health and safety.

B. Approved Privacy Codes

Under the act, organisations have the option of either (1) developing a self-regulatory code approved by the Privacy Commissioner and which does not include a complaints resolution process, in which case the organisation is subject to a complaints resolution process operated by the commissioner; (2) developing a self-regulatory code including a complaints resolution mechanism, again subject to approval by the commissioner); or (3) complying with the NPPs and being directly subject to the complaints resolution process operated by the commissioner.

A self-regulatory code may apply to an organisation, an industry sector or a profession, or specified classes of industry sectors or professions, and may deal with all, or a specified type, of personal information. If an industry body or organisation proposes to develop a self-regulatory code, before that code will be effective under the

act as an "approved privacy code," it first must be approved by the Privacy Commissioner.

Section 18BB of the act mandates that the commissioner must be satisfied that (1) the code incorporates all of the NPPs or sets out obligations that "overall, are at least the equivalent of the obligations" in the NPPs; (2) the code specifies the organisations bound by the code or a way of determining the organisations that are, or will be, bound by the code; (3) the code binds only organisations that consent to be bound; (4) the code sets out a procedure by which an organisation may cease to be bound by the code and when the cessation takes effect; (5) if the code includes a complaints resolution mechanism, that specified criteria (set out in Section 18(3)) of the act are satisfied with regard to that mechanism; and (6) members of the public have been given adequate opportunity to comment on a draft of the code.

An industry peak body or individual organisation that chooses to develop its own privacy code can to some extent tailor the content of the code to suit its specific information handling acts and practices. However, the overriding requirement that an approved privacy code incorporate obligations that, overall, are at least the equivalent of the obligations set out in the NPPs, requires organisations to consider carefully the precise form of any modifications incorporated in the code. It is, of course, possible that some industry or professional associations will wish to develop NPPs that provide for more onerous obligations than those of the NPPs.[8]

C. Breach of Approved Privacy Code

The trigger for the remedial and protective mechanisms provided under the private sector regime is an interference with the privacy of an individual.

An act or practice of an organisation is an "interference with the privacy of an individual" if it breaches—that is, contrary to or inconsistent with—(1) an approved privacy code that binds the organisation; or (2) the NPPs, in circumstances where an approved privacy code does not exist or does not apply; or (3) in the case of a contracted service provider for a commonwealth contract, a provision of that contract which, in effect, imposes an alternative obligation on that contracted service provider to those specified in the NPPs (or any approved privacy code); and (4) the act or practice relates to personal information that relates to the individual.

Disclosures by organisations for the purposes of enabling the National Archives of Australia to determine whether to accept or arrange custody of a record for the purposes of the Archives Act 1983 are excluded from the definition of a breach of the NPPs or an approved privacy code.

Also exempted from the definition of a "breach" of the NPPs and approved privacy codes are acts or practices engaged in outside Australia and the external territories that are required by the applicable law of a foreign country. Sections 6A(4) and 6B(4). Section 13D reinforces or duplicates the effect of these sections by providing that these acts or practices are not "interferences with privacy." The private sector regime affects overseas acts and practices of organisations with a "link" to Australia and which relate to personal information about Australian citizens or persons whose continued presence in Australia is not subject to any time limit imposed by law. Section 5B sets out the circumstances in which a link is established for the purposes of the extra-territorial operation of the private sector regime.

Sections 13A(2) and 13E of the act make clear that:

- It is irrelevant to determining whether an act or practice of an organisation is an interference with privacy that the organisation is also a credit reporting agency, credit provider or file number recipient. In other words, an act or practice of an organisation may be an interference with privacy both for the purposes of the Privacy Act regime and for the purposes of

8. The Revised EM cites the example of medical professionals who may wish to give effect to long-standing obligations of client-doctor confidentiality.

the regime established by the Private Sector Act if the organisation is a credit reporting agency, credit provider, or file number recipient;[9] and

- The exceptions from the scope of acts and practices which are "interferences with privacy" provided in relation to related bodies corporate, changes in partnerships, and overseas acts in compliance with foreign laws do not affect obligations applicable to credit reporting agencies, credit providers or file number recipients.

D. Complaints and Investigations

An act or practice which an individual believes to be an interference with their privacy may form the basis of a complaint. Some complaints by individuals may be finally resolved directly between the individual and the organisation concerned. The private sector regime positively encourages this approach, which means that many privacy complaints are dealt with without resort to any formal complaints resolution process.

1. Complaint Resolution Process

If individuals cannot resolve their complaint directly with the organisation, they can attempt to resolve the complaint through a complaints resolution process established under an approved privacy code (if any) or by referring their complaint to the Privacy Commissioner for investigation.

If the organisation is bound by an approved privacy code with a procedure for an adjudicator, the individual must first pursue that procedure, unless the approved privacy code itself provides that the Privacy Commissioner is to be the adjudicator. The commissioner is not empowered to investigate a complaint in the first instance if the individual has not complained to the organisation concerned, unless the commissioner decides it was not appropriate for a complaint to be made to the organisation.

Apparently this provision applies regardless of whether the organisation is bound by an approved privacy code including a complaints-handling process. Approved privacy codes will themselves require that individuals must first have attempted, without success, to resolve their complaints directly with the organisation before they will be entitled to have their complaints investigated by a code adjudicator.

Code adjudicators must refer all complaints about acts and practices by contracted service providers for commonwealth contracts to the Privacy Commissioner for investigation, regardless of any provision in the approved privacy code which purports to give it power to deal with the matter. Presumably, a code that included such a provision would not be approved by the commissioner.

Section 36 of the act provides for a representative complaint to be made to the commissioner by an individual where an act or practice may interfere with the privacy of two or more persons, including the individual making the complaint. It remains to be seen whether self-regulatory privacy codes submitted for approval to the commissioner will seek or will be required to accommodate representative complaints.

Part V of the Privacy Act, as amended by the Private Sector Act, contains detailed provisions concerning the procedural obligations and powers of the Privacy Commissioner with regard to the investigation of complaints, as well as acts and practices generally. These powers extend to requiring the production of documents and to examining witnesses on oath.

2. When Commissioner Must Investigate

The threshold requirements before the Privacy Commissioner must investigate an act or practice are (1) a complaint must have been made by an individual about an

9. Section 6(7) also makes clear that a complaint that an act or practice breaches an NPP may also be a complaint that the same act or practice is a credit reporting infringement or a complaint in relation to handling of TFN information. An organisation accordingly might be the subject of more than one adverse finding. *See* Revised EM, Items 57-59.

act or practice, and (2) the commissioner must have decided that the act or practice may be an interference with the privacy of an individual.

3. When Commissioner May Investigate

The commissioner also has the discretion to investigate an act or practice on his own initiative without a complaint having been made if he thinks it is desirable. There are reporting requirements when the commissioner investigates in the absence of a complaint. In certain circumstances, for example, if the commissioner forms the view that a complaint can and could be dealt with more appropriately by the Human Rights and Equal Opportunity Commission, the commissioner may transfer the complaint. In other circumstances, the commissioner must cease or discontinue in part an investigation and refer the matter to the Commissioner of Police or Director or Public Prosecutions.

4. Terminating Investigations

The commissioner may decide not to investigate or not to investigate further if the commissioners decides the acts or practices (1) are not interferences with privacy; or (2) the complaints are frivolous vexatious or lacking in substance; or (3) the complaints are being adequately dealt with by alternative remedies provided under commonwealth, state or territory law; or (4) if the commissioner decides that a complaint has been dealt with adequately by an organisation or the organisation has not yet had an adequate opportunity to deal with the complaint.

5. Public Interest Determinations

Section 72 of the act provides for applications to be made by organisations for determination as to whether particular acts or practices breach the NPPs or an approved privacy code. If such an application has been made, the commissioner may defer an investigation in relation to the particular act or practice until the commissioner has dealt with the application, provided an individual's interests will not be prejudiced by the deferral.

6. "Guiding Principle"

Section 29(a) of the act requires that the commissioner must have due regard in performing functions and exercising powers "for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the recognition of the right of government and business to achieve their objectives in an efficient way."

Section 18BB(3)(c) of the act requires that a complaints resolution process under an approved privacy code also must oblige the code adjudicator to have regard to the same matters.

E. Determinations

1. The Determination

Following the completion of an investigation of a complaint by either the Privacy Commissioner or a code adjudicator, a determination will be made. Section 18BB of the act provides that a complaints handling process under an approved privacy code must confer powers on the code adjudicator with respect to determinations which are the same as those conferred on the commissioner and set out the means by which, under the approved privacy code, the organisation is bound to comply with that determination.

The determination includes a statement of the findings of fact on which the determination is based, which is important in any subsequent review of the determination. A determination results in either a dismissal or a finding that the complaint is substantiated. When a complaint is found to be substantiated, declarations can be made that remedial steps should be taken, including payment of compensation for loss or damage, extending to injury to the complainant's feelings or humiliation suffered by the complainant. Section 52.

2. Review of Determination

A person aggrieved by a determination of a code adjudicator, except where the code adjudicator is the commissioner, may apply to the commissioner to review the determination. Section 18BI. The review includes any finding, declaration, order or direction included in the code adjudicator's determination. A determination by the commissioner is a judicially reviewable decision.

Approved privacy codes must include reporting requirements in accordance with Section 18BB(3)(h)-(l) of the act, which complement the supervisory function and powers conferred on the commissioner with respect to approved privacy codes. These powers extend to a review of outcomes of complaints dealt with by code adjudicators appointed under approved privacy codes.

F. Enforcement

No penalty attaches directly to a failure to comply with a determination by a code adjudicator or the commissioner, which is not binding or conclusive on the parties. If a determination is not complied with by an organisation, the individual concerned, the commissioner or the relevant code adjudicator may apply to the Federal Court or the Federal Magistrates Court for enforcement of the determination.

The court is required to deal with the matter by way of hearing de novo, and when conducting such a hearing, to have due regard to the "guiding principle" noted above. The court may receive in evidence copies of the commissioner's or code adjudicator's reasons, documents that were before the commissioner or code adjudicator, and records of appearances before the commissioner or code adjudicator.

KEY ISSUES

A. Legal Profession

The act has some potentially far-reaching implications for the legal profession in Australia.

1. Subject to Act?

A lawyer practising as a sole practitioner may be subject to regulation under the act as an organisation in relation to the conduct of his or her business activities as a lawyer, which would include acting for clients in the course of litigation. It is likely that many sole practitioners will fall within the small business exception and for that reason may not be regulated under the act. Partnerships, particularly the larger law firms, will generally not come within the small business exception.

2. Conduct of Litigation

The process of litigation invariably involves aspects of collection, use, storage and disclosure of personal information. While the act contains a number of specific exemptions in relation to, for example, information required by law or information related to legal proceedings, it does not contain any sort of general exemption for people or organizations—such as law firms and their clients—who may be acting in or otherwise engaged in the course of litigation.

In effect, this means that lawyers and their clients who may be engaged in the preparation, investigation or conduct of legal proceeding in Australia, including any persons engaged by lawyers or their clients, such as process servers or private investigators, are subject to the general requirements of the act, subject to any applicable exceptions, including the NPPs.

The practical effect of these requirements in the particular context of litigation remains somewhat unclear. The Privacy Commissioner has not released any guidelines or information sheets on the subject. However, the commissioner is considering the issue. In the interim, it is important for lawyers to be aware that a potentially vast array of personal information collected in the course of preparing or conducting litigation now needs to be managed in accordance with the requirements of the act.

The act, or more precisely the NPPs, contain a number of specific exceptions relevant to the conduct of litigation. For

example, an organisation can legitimately refuse an individual access to personal information the organisation holds about them, as set out in NPP 6(1) where the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery (NPP 6.1(e)); and (2) where denying access is required or authorised by law (NPP 6.1(h)).

Similarly there is an exception to the general prohibition on the collection of sensitive information (NPP 10.1) where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim. There is no corresponding exception in relation to the requirements of NPP 1.3 (or, where applicable, NPP 1.5) to ensure that individuals have been made aware of certain matters where personal information is collected about them. However, the obligation under NPP 1.3 is to take reasonable steps to make an individual aware of the required matters at or before the time of collection or, if that is not practicable, as soon as practicable after collection. What is practicable will depend on the specific circumstances of each case. It may be that in some situations it will not be practicable to make a disclosure until well after the time the personal information was collected or it may be that in certain circumstances it is not practicable to make a disclosure at all.

Key issues for lawyers involved in the conduct of litigation in Australia include the following.

a. Client Legal Privilege

As a general rule, once privilege is lost, it cannot be re-stated. Accordingly, one of the issues for lawyers that may arise under the act is the question of access to personal information that is or may be the subject of a claim for privilege. There is no specific provision in the act for denying access on the basis of a claim for client legal privilege. However, client legal privilege should provide a reasonable basis for asserting that a denial of access is required or authorised by law (NPP 6.1(h)). Similarly, the assertion of the duty of confidentiality owed by a lawyer to his client also should be sufficient to deny access on the same basis.

b. Use of Private Investigators

It is reasonably common for lawyers involved in the preparation of certain types of litigation—for example, that arising from insurance claims—to retain the services of a private investigator to assist in the collection of background information and evidence. However, to the extent that any of the information collected is personal information, this will give rise to a number of specific obligations under NPP 1. It is now necessary to ensure that the only personal information collected is that necessary for the purpose of the litigation (NPP 1.1). It is also necessary to ensure that the information is not collected in an unreasonably intrusive way (NPP 1.2).

One of the difficult issues is the extent to which a private investigator is obliged to take reasonable steps to ensure that the individual about whom the information is being collected is aware of, amongst other things, the identity of the private investigator collecting the information, the fact that they can access the information, and the purpose for which the information is being collected, in accordance with NPP 1.3.

The key question appears to be whether it is impracticable in these circumstances for the private investigator to make an NPP 1.3 disclosure at or before the time of collection and when it will be practicable to make the disclosure after the collection. Given that any disclosure prior to or during collection of information will in all likelihood frustrate the activities of the private investigator, it may be possible to argue that it is not practicable to make a disclosure at or before the time of collection. When it will be practicable to make a disclosure after collection will depend on the specific circumstances of each case.

B. Retail Banks and Credit Providers

For credit reporters and credit providers

subject to regulation under Part IIIA of the act, the broad philosophy underlying the private sector regime is not unfamiliar: certain information must be handled only in a prescribed manner.

Credit reporting agencies and credit providers remain subject to Part IIIA of the act. Moreover, the obligations of credit providers apart from the requirements of the act will continue to apply. For example, in a particular case, a bank may not be prohibited by the NPPs from disclosing personal information, but the bank's duty of confidentiality at common law may still prevent the disclosure of the information.

However, the private sector regime impacts not just on a specific category of information handled by credit reporters and credit providers, but on all aspects of personal information handling. A vast array of personal information needs to be managed in accordance with the private sector regime's requirements, and this will impact both front and back-end operations of credit providers.

Key issues for retail banks and other credit providers arising from the private sector regime include:

- the impact of dual sanctions for practices which are affected both by the credit reporting regime under Part IIIA and the private sector regime;
- the interaction of the NPPs and any applicable codes of conduct, such as the Code of Banking Practice, which includes specific privacy requirements;
- protocols for cross-selling products and the implications of the related body corporate exemption across corporate groups;
- relationships with authorised representatives, franchisees and contractors with whom personal information is exchanged;
- account systems implications and the capacity for systems to accommodate appropriate security measures for personal information, to flag sensitive information for special protection and retrieve information for access and correction purposes; and
- the implications of mergers and acquisitions requiring combination of discrete sets of personal information.

C. Health Industry

As stated above, the act creates a special category of personal information, termed "sensitive information," and it gives greater protection to sensitive information by placing stricter limits on how it is collected and handled by private sector organisations. Health information is a form of sensitive information.

The act defines "health information" as:

> (a) information or opinion about:
>
> (i) the health or a disability (at any time) of an individual; or
>
> (ii) an individual's expressed wishes about the future provision of health services to him or her; or
>
> (iii) the health service provided, or to be provided, to an individual;
>
> that is also personal information; or
>
> (b) other personal information collected to provide, or in providing, a health service; or
>
> (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.

It should be noted that sub-paragraph (b) of this definition means that some types of personal information to be categorised as sensitive information if collected incidentally to the provision of a health service—that is, the collection occurs "in providing" a health service." However, it is important also to note the general provision under Section 16B that the act applies only to the collection of personal information if the information is collected for inclusion in a record or a generally available publication and only to personal information collected by the organisation which is held in a record.

The act defines "health service" as:

> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
>
> (i) to assess, record or maintain or improve the individual's health; or
>
> (ii) to diagnose the individual's illness or disability; or
>
> (iii) to treat the individual's illness or

> disability or suspected illness or disability; or
>
> (b) the dispensing on prescription of a drug or medicine or preparation by a pharmacist.

In addition to the special protection attaching to health information as "sensitive information," the NPPs also deal specifically with health information in the context of its use and disclosure for research and in the course of treatment of individuals, and they include a number of measures intended to balance the restrictions set out in the NPPs with the necessity for health services and research in relation to health to be conducted.

Key issues for the health industry in relation to the private sector regime include:

- the scope of the definition of "health service"; how far does it extend beyond medical practitioners and pharmacists?
- the impact of dual or multiple regulatory regimes affecting health service providers;
- the effectiveness of existing practices for procuring client/customer/patient consents;
- the adequacy of any existing procedures guiding decisions about collection where there is a serious threat to life or health of individuals (or other exceptional circumstances);
- research guidelines and the circumstances in which non-identifiable information only should be collected;
- limitations on direct marketing specifically applicable to sensitive information, and the potential segmenting of databases of personal information this may require;
- the implications of access requirements under the private sector regime for previous limitations on rights of patient access to medical records;[10] and
- procedures for exchange of personal information within treating teams which do not impede efficiency.

D. Superannuation, Insurance and Funds Management

Financial services providers, such as banks, insurers and superannuation funds, hold a vast amount of personal information as a function of their business. Technological advances have given businesses the capability to break down this customer information into its components and then recombine the information for other purposes. An example of this is information provided to a bank in relation to a loan application, such as age, address, marital and family status, which could be recompiled to propose new loans, investments, life and general insurance and superannuation products.

1. Superannuation

Superannuation trustees have limited privacy duties in respect of the personal information of the members of the superannuation fund outside of the act. Trustees are in a fiduciary relationship with the members of the fund and are subject to the usual fiduciary duties, including to act in the best interests of members. If a trustee breaches the privacy of a member of the fund to the member's damage, or the trustee uses the breach to obtain a benefit, the trustee could be liable for a breach of fiduciary duty.

In addition to fiduciary duties, superannuation trustees are subject to detailed disclosure and reporting rules under the Superannuation Industry (Supervision) Act 1993, which supplements the general law rights of beneficiaries in relation to information held by trustees. Superannuation trusts also are subject to the tax file number privacy principles contained in the Privacy Act, which place restrictions on the collection, use and storage of tax file numbers by the superannuation industry.

Moreover, trustees could be liable for a breach of confidence where they have disclosed personal information of members to third parties. The requirements to establish

10. *See* Breen v. Williams (1996) 186 C.L.R. 71. State and territory legislation also impacts on this issue, for example, Section 120A of the Mental Health Act 1986 (Vic), Health Records (Privacy and Access) Act 1997 (ACT), and the Health Records Act 2001 (Vic).

a breach of the equitable duty of confidence are: (1) The information must be of a confidential nature. (2) There must be a relationship of confidence. (3) There must be an unauthorised use or disclosure of the information to the detriment of the person who provided the information. As a result, the superannuation industry already had some experience in dealing with privacy issues prior to the commencement of the Private Sector Act.

Many of the issues impacting on retail credit providers also affect superannuation entities. Other key issues include:

- reviewing relationships with employers which disclose information to entities where employers may be subject to the employee records exemption;
- consideration of procedures to control communications by trustees with spouses or former spouses of members; and
- controlling disclosures of personal information to and collection of personal information from advise acting in connection with the operation of a superannuation fund.

2. Insurance

Contracts between insurers and individuals are contracts of utmost good faith. This means that the insured individual has a duty to disclose to an insurer, before the contract is entered into, every matter known to the insured, or that a reasonable person in the circumstances could be expected to know, relevant to the insurer's decision whether to accept the insurance risk, and if so, on what terms. This obligation is reinforced by the Insurance Contracts Act 1984.

One result of these obligations is that insurance companies are privy to vast amounts of personal information about individuals, and in many cases, particularly in the life insurance and health insurance areas, this information is of a highly sensitive nature and which the individual insured would not wish to be disclosed to other parties. The impact of the private sector regime is felt more acutely by life insurance and health insurance companies because they typically are involved in the collection of significant amounts of health information, which falls within the definition of sensitive information.

The general insurance industry has recognised for some time the importance of privacy principles. It is the first group to have a privacy code approved by the Privacy Commissioner under the act—the General Insurance Privacy Code, approved 17 April 2002.

Key issues for life and health insurers in relation to the private sector regime include:

- the interaction of customer's duties to disclose with requirements for consent under the private sector regime where sensitive information is collected;
- the specific limitations on the "reasonable expectation" qualification (NPP 2) where sensitive information is used for a secondary purpose (when will the secondary purpose be "directly related" to the primary purpose?);
- (in the future) the possible impact of the scope of regulation of sensitive genetic information. This is a controversial issue that will be subject to a review by the Australian Law Reform Commission and the Australian Health Ethics Committee. For this reason, genetic information was not dealt with in the act, as the government preferred to wait for the publication of the recommendations of this inquiry.[11]

3. Funds Management

As with superannuation trustees, the relationship between funds managers and their members gives rise to fiduciary duties on the part of the responsible entity of the fund. The duties are supplemented by the

11. The Australian Compensation and Consumer Commission has granted authorisation to a proposed agreement by life insurers that they will not initiate or induce applicants for life insurance to undergo genetic testing for a period of two years. This agreement does not deal expressly with the use of existing genetic information. *ACCC Authorises Life Insurance Bar on Genetic Testing*," release by ACCC, 22 November 2000, available at www.accc.gov.au/docs/a30200_a30201.pdf. A press release is available at http://www.accc.gov.au//fs-search.htm, then enter key words "genetic,tsting."

Corporations Law, and in particular Section 601C(1)(c), which requires responsible entities to act in the best interests of members, and Section 601FC(1)(e), which prohibits responsible entities from making use of information acquired through being a responsible entity in order to gain an improper advantage for itself or another person or to cause detriment to the members of the scheme.

Key issues for funds managers include:

- identifying means of regulating relationships with intermediaries who deal directly with investors;
- assessing the implications of transitions to fund structure, roll-overs, and acquisitions of relevant entities; and
- defining access and correction obligations with respect to personal information and the scope of exemptions provided for evaluative information generated in connection with a commercially sensitive decision making process.

E. Marketing Activities

1. General

Personal information is central to many marketing activities, whether it is used for simple procedures, such as providing contact details for businesses' customers, or more complex activities, such as analysing customers' spending and leisure habits in order more successfully to tailor products to the core market of a business.

Key issues for marketing activities of organisations include considering:

- the means by which call centres and market research organisations comply with disclosure requirements at the point of collection, and the extent of their obligations to disclose the identity of organisations to whom they disclose the results of their research and the purpose for which those organisations use the data;
- compliance issues where standard form scripts are used for the purpose of making disclosures and obtaining consent;
- whether it is "practicable" to disclose purposes of use before collection of personal information, and, if not, when it is practicable to make that disclosure;
- the scope of the obligations of organisations collecting data from market researchers and call centres to satisfy themselves that disclosures have been made for the purposes of NPP 1.5 (what are "reasonable steps"?); and
- the responsibilities of organisations which outsource some marketing and call centre functions to overseas agencies, given the provisions of NPP 9, which affect transborder data flows.

2. Direct and Telemarketing

The use of personal information for the direct marketing of products to consumers has been specifically dealt with in the Act under NPP 2.1(c), which requires organisations to consider:

- amendments to written direct marketing communications to ensure appropriate opt-out notice and contact details;
- processes to honour opt-out requests of recipients of direct marketing communications;
- the impact of the related body corporate exemption on direct marketing practices;
- development and maintenance of procedures for excluding collection of sensitive information from material collected in the course of direct marketing; and
- investigating the potential for call centre contacts with individuals and point of sale forms to provide the means of obtaining consents.

The privacy principles contained in the Australian Direct Marketing Association Code of Practice are based on the NPPs. The association also has an independent code authority to deal with any complaints against its members, which it has indicated it will seek to have approved as a code adjudicator under the act. The association also offers a service known as the "Do Not Mail/Do Not Call" file, which apparently cleans the databases of member organisations of the names of consumers who have registered not to receive direct marketing offers by mail or telephone.

3. E-commerce and Online

One of the most commonly quoted impediments to achieving the full potential of online services, and in particular the full development of electronic commerce, is the lack of consumer confidence in the privacy and integrity of communications online.

Personal information about consumers is of utmost importance for the business models of many online companies operating on the Internet. The use of such personal information is seen to be vital for the marketing of many products online, as well as for the tailoring of those products to the specific preferences of individual consumers. Advertisers on the worldwide web, and in particular those utilising click-through banners and pop-ups, rely on personal information collected by websites to customise their marketing, placing pressure on websites to enable them to collect personal information collected when customers access their advertisements. Information as to the browsing habits and spending patterns of consumers online also is valuable for both offline and online organisations. In fact, for many online companies their customer database is one of their most valuable assets.

An e-privacy report in 2000, which canvassed 100 of the top websites visited by Australians, found that 72 percent of the sites collected personal information from consumers who visited the site, while only 28 percent of those sites told users that specific personal information was being collected. The survey found that 43 percent of the sites that collected personal information did so without users actively providing it.[12] This raises the thorny question of the adequacy of "consents" obtained using click-through processes or passive displays that may not adequately be brought to the attention of users.

One potential source of an applicable code for online businesses is the Internet Industry Association (IIA) Internet Industry Code of Practice. Section 8 of that code, entitled "Collection and Use of User Details," commits signatories to complying with the Privacy Commissioner's NPPs. It also contains additional obligations in relation to the protection of a user's personal information. The IIA is currently in the process of finalising a privacy code and will then seek to have that code approved by the Privacy Commissioner. Its code relies on a seal program, which will, according to the IIA, be the first government-backed, industry-developed privacy seal in the world.

Key issues affecting e-commerce and online services include:

- limits of the definition of personal information: e-mail addresses, web bugs and cookies,[13] and the consequences of their combination with other sources of information in databases or back up systems;
- the potential for implementation of a private sector compliance regime to assist in curbing online fraud and identity theft by promoting more rigorous identification processes and access controls;
- apparently "anonymous" transactions in which an individual's identity is in fact recorded (this will be an acute issue for organisations unfamiliar with their system functions and capability);
- the challenge of accommodating functional and stylistic requirements in the course of developing privacy compliant websites with adequate notices and provision for obtaining consent;
- hypertext links, their adequacy as a means of displaying disclosure material and disclaimers, and the "timing" of their deployment;

---

12. Andersen Legal/Arthur Andersen, *Internet Privacy Survey 2000—A Survey of the Privacy Practices of Australia's Most Popular Websites*, 26 October 2000, available through Google at http://www.google.com/search?q=cache:Vy5km9 qJv28C:www.iia.net.au/aasurvey.PDF+internet+privacy+survey+2000&hl=en&ie=UTF-8. A press release from the Internet Industry Association is available at http://www.iia.net.au/news/aasurvey.html.

13. Issues arising from the use of cookies are discussed in some detail in Sections 2.33-2.57 of *Cookie Monsters? Privacy in the Information Society*, a report by the Senate Select Committee on Information Technologies, November 2000.

- the form and role of security statements and privacy policies and the private sector regime's "opt-in" provision as compliance mechanisms and a means of "credentialing" an organisation;
- the extent to which non-governmental organisations which provide privacy accreditation services (for example, TRUSTe or the BBBOnline Privacy Program run by the Council of Better Business Bureaus) will benefit from the implementation of the private sector regime;
- the significance of the "technology-neutral" approach of the private sector regime in light of the absence of firmly established global standards for online security;
- procedures for controlling offline handling of personal information obtained by organisations through their online services;
- the viability of an online or partly online complaints resolution process;
- determining the location of an organisation for the purposes of determining whether NPP 9 requirements with regard to transborder data flows are attracted; and
- the outcome of the pending review of the private sector regime by the European Union, and the consequences for online business of an unfavourable finding.

The Privacy Project

The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Requirements

The Privacy Rule contains a maze of mandates and exceptions requiring that entities covered by HIPAA need the best of health care counsel

By Nancy A. Lawson, Jennifer M. Orr and Doedy Sheehan Klar

THE Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub.L. No. 104-191) was created and enacted in response to the health care industry's request for standardization, as a remedy for increasingly frequent health care privacy breaches, and as an effort to halt steady increases in health care costs. It received bi-partisan Congressional and industry-wide approval and was signed into law on August 21, 1996.

HIPAA's enactment was without much fanfare. Most attention focused on the fact that HIPAA (1) amended the Employees Retirement Income Security Act (ERISA) to limit health plans' ability to use pre-existing condition coverage exclusions and (2) barred discrimination by health plans in a variety of areas.

IADC member Nancy A. Lawson is partner in Dinsmore & Shohl LLP in Cincinnati, where she concentrates in business litigation, products liability and general civil litigation. She has a B.A. from Skidmore College (1970) an M.Ed. from Boston University (1971) and a J.D. from the University of Toledo (1975).

Jennifer M. Orr is an associate at Dinsmore & Shohl. She is a graduate of Miami University (B.A. 1995) and the University of Akron (J.D. 1998), and she concentrates in litigation and health care law.

IADC member Doedy Sheehan Klar is assistant general counsel of Alcon Laboratories Inc. in Fort Worth, Texas, dealing with litigation and advertising and regulatory law. She earned a B.S. in 1977 from the University of Texas at Dallas and a J.D. in 1990 from St. Mary's University.

A. Privacy Rule

More important for defense counsel, Title II of HIPAA, denominated "Administrative Simplification," required Congress to pass privacy, security and electronic health care transaction standards to regulate the use of health information transmitted electronically, which, by regulation, now has been expanded to encompass health information in any form or medium.

In a nutshell, the HIPAA standards, when fully implemented, are expected to and will:

- simplify the administration of health insurance claims and the costs associated with those claims by encouraging the promulgation of national standards;
- give patients more control over and access to their medical information;
- protect individually identifiable health information from real or potential threats of disclosure through the setting and enforcing of standards; and
- improve efficiency in health care delivery by standardizing electronic data interchange (EDI).

Title II stated that if by December 1999, Congress failed to pass meaningful health privacy legislation, with the input of the U.S. Department of Health and Human Services (HHS), then HHS was required to assume the responsibility. HHS's recommendations regarding federal privacy legislation were submitted to Congress in 1997,

but Congress ultimately failed to act. As a result, HHS published the Standards for Privacy of Individually Identifiable Health Information, known as the Privacy Rule, in December 2000.[1]

In March 2002, after receiving, reviewing and responding to more than 60,000 public comments on the rule, HHS issued proposed modifications. These changes were intended to alleviate problems with the original "final" rule that unintentionally impeded patient access to health care, while still maintaining the requirements for the privacy of individually identifiable health information. Primarily, the changes included: (1) eliminating the patient "consent" requirement, (2) modifying the definition of "marketing," (3) providing allowances for "incidental uses and disclosures" of protected health information, and (4) allowing additional time for compliance with the cumbersome business associate provisions.

Finally, in mid-August 2002, after an additional comment period, HHS issued its final version of the Privacy Rule and thereby finalized the groundbreaking and controversial federal privacy regulations. For all intents and purposes, the proposed changes in the March 27, 2002, amendment were adopted. Covered entities are required to comply with the Privacy Rule's requirements on or before April 14, 2003, with the exception that small health plans are given an additional year to comply. Small health plans, by statute, are those with fewer than 50 participants and/or plans with annual receipts of $5 million or less.

B. Transactions and Code Sets Rule

The Privacy Rule represents only one portion of HIPAA Administrative Simplification. In fact, well before the Privacy Rule was finalized, HIPAA-covered entities and their business associates already were implementing the Standards for Electronic Transactions, known as the Transactions and Code Sets Rule, as compliance with that rule originally was required on or before October 16, 2002, except for small health plans. In response to requests from many sectors of the health care industry, Congress passed the Administrative Simplification Compliance Act (ASCA), which allows most covered entities to request a one-year extension until October 16, 2003.

If no ASCA compliance plan or extension request was submitted on or before October 15, 2002, it is assumed that the covered entity is in compliance with the Transactions and Code Sets Rule. HIPAA penalties for non-compliance can be assessed against entities that are not transmitting HIPAA standard transactions on October 16, 2002, including possible exclusion from Medicare.[2]

C. Security Rule

HIPAA Administrative Simplification also calls for a Security Rule to be promulgated. One difficulty with compliance is that no final Security Rule had been issued as of the fall of 2002. Under HIPAA, and the proposed 1998 proposed Privacy Rule, certain security measures are required to be implemented. Fortunately, all indications are that the final Security Rule will not be significantly different from the proposed rule, so covered entities and their business associates can and should use the proposed rule as a guide for complying with the Privacy Rule's security mandates.

D. The Five Principles

There are five principles of fair information practices that underlie all the HIPAA rules.

---

1. The Privacy Rule and its Comments are codified at 45 C.F.R. Parts 160 and 164. The full text of the regulations and guidance on HIPAA implementation are available at aspe.os.dhhs.gov/admnsimp/ and www.hhs.gov/ocr/hipaa. *See also* Richard L. Antognini, *The Law of Unintended Consequences: HIPAA and Liability Insurers*, 69 DEF. COUNS. J. 296 (2002).

Federal and state statutes creating additional obligations for the handling of records and other information pertaining to individually identifiable health information, such as mental health information and AIDS, drug and/or alcohol treatment information, are beyond the scope of this article.

2. The model compliance plan promulgated by the Center for Medicare and Medicaid Services (CMS) is available at www.cms.gov/hipaa/hipaa2/ASCAForm.asp.

First is the principle of openness, or notice, which has as its focus assuring that the existence and purposes of record-keeping systems are publicly known. Second, the principle of individual participation, or access, states that individuals should have the right to see their records and assure the accuracy, completeness and timeliness. Third, the security principle stands for the proposition that there should be reasonable safeguards in place for protecting the confidentiality, integrity and availability of information. The fourth principle is that of accountability, or enforcement, meaning that violations of the HIPAA rules should result in reasonable penalties, and mitigation should be permitted and encouraged. Finally, with respect to fair information practices, there should be limits placed on collection, use and disclosure of information (or choice). Information should be collected only with the knowledge of the individual, it should be used only in ways that are relevant for the purposes for which it is being collected, and it should be disclosed only with consent/notice or authority.[3]

E. The Road Ahead

It is within this regulatory landscape that the Privacy Rule was constructed. Compliance with the rule on or before April 14, 2003, will require covered entities and those who advise them to be intimately familiar with the basic terminology and requirements of the rule and take the necessary steps to implement its requirements into their business practices. Covered entities would be wise to establish an integrated approach to HIPAA's Administrative Simplification rules for transactions, privacy and security, as such integration and understanding is essential to successful, cost-effective compliance initiatives.

PRIVACY RULE BASICS

A. What the Rule Does

The Privacy Rule is composed of two regulatory subparts (45 C.F.R. Parts 160 and 164, and it is centered on one basic concept: covered entities (and by extension, their business associates) are prohibited from using or disclosing protected health information (PHI) unless they follow the Privacy Rule and strictly adhere to its requirements. 45 C.F.R. § 164.502 states: "A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this chapter."

What does this mean? As a starting point, the Privacy Rule calls for the following:

- It limits the ability of covered entities and their business associates to use or transmit PHI without specific advance notification of the covered entity's privacy practices to the individual whose information is at issue, and, in certain circumstances set out in the rule, the advance authorization of the individual for a particular use or disclosure.
- It grants covered entities a variety of exceptions from the advance authorization requirement, as explained below.
- It requires that, even when permitted to disclose protected health information, covered entities make reasonable efforts to limit disclosure to the "minimum necessary" to accomplish the intended purpose of the use or disclosure. The rule sets out a variety of exceptions to the "minimum necessary" standard.
- It allows individuals to inspect, copy and amend their protected health information, where specific criteria are satisfied, and it also grants individuals the right to request an accounting of unauthorized uses and disclosures of their protected health information.
- It allows individuals to request restrictions on the uses or disclosures of protected health information for which the

3. These principles were discussed by William R. Braithwaite, M.D., Ph.D., colloquially referred to as "Dr. HIPAA," at the HIPAA Summit West in San Francisco on March 14, 2002. Dr. Braithwaite was directly involved in the drafting of the Privacy Rule while working for the government. Now, as a private consultant with PriceWaterhouseCoopers, he advises health care entities and assists with HIPAA compliance.

covered entity may otherwise possess the right to use or disclose. The covered entity does not have to agree to the restriction. If the covered entity agrees, then it must document compliance with the restriction.

B. Application of the Rule

The Privacy Rule applies to all "covered entities," which under 45 C.F.R. § 160.102 include: (1) health plans, (2) health care clearinghouses and (3) health care providers who transmit any health information in electronic form in connection with a transaction covered by HIPAA. It is worth noting that health care providers who do not submit HIPAA transactions in standard form become covered by this rule when other entities, such as a billing service or a hospital, transmit standard electronic transactions on their behalf. In addition, business associates of covered entities who use, disclose or have access to protected health information are indirectly affected by the Privacy Rule's mandates.

Necessarily, then, the next logical inquiry is to determine what transactions are considered HIPAA transactions for purposes of deciding whether a health care provider is a covered entity. "Transactions" are the transmission of information between two parties to carry out financial or administrative activities related to health care. 45 C.F.R. § 160.103.

The following types of information transmissions are considered HIPAA transactions:

- Health care claims or equivalent encounter information;
- Health care payment and remittance advice;
- Coordination of benefits;
- Health care claim status;
- Enrollment and disenrollment in a health plan;
- Eligibility for a health plan;
- Health plan premium payments;
- Referral certification and authorization;
- First report of injury;
- Health claims attachments; and
- Other transactions that the HHS Secretary may prescribe by regulation.

Under the Transactions and Codes Sets Rule, standards have been established for all these transactions except for the first report of injury and health claims attachments. Standards for these two categories of HIPAA transactions are expected to be proposed soon. As a result, it is necessary for covered entities to consider relevant portions of the Transactions and Code Sets Rule that may affect their implementation of the Privacy Rule's requirements.

For example, the following electronic activities would likely not be considered HIPAA "transactions" in and of themselves. Health care providers conducting these activities, and only these activities, may well fall outside of the definition of "covered entity:"

- Sending a facsimile to another treating physician that contains PHI;
- Sending an e-mail to another physician asking a question about a patient;
- Saving a medical record to disk and mailing it to another treating physician; and
- Using the Internet to transmit required information to the government.

The Privacy Rule does not apply directly other than to "covered entities" identified above. The business associates of covered entities will necessarily, by contract, be obligated to comply with certain aspects of the Privacy Rule, but covered entities are the only ones against which HIPAA penalties may be levied for violation of and/or non-compliance with the Privacy Rule.

The entities to which the Privacy Rule does not apply are: (1) non-covered entities and (2) health care providers who do not electronically submit HIPAA transactions. For example, some solo practitioners and some small health plans that do not submit claims electronically and have obtained waivers for submitting Medicare claims in paper format arguably would not be considered "covered entities."

The determination of "covered entity" should be made on a case-by-case basis. For instance, the final Security Rule, when issued, may well apply to health care providers not now considered "covered enti-

ties" under the Privacy Rule. The services provided by health care providers should be analyzed carefully to ensure that other requirements and laws (such as "more stringent" state laws) do not bring non-covered entities within the Privacy Rule.

C. What Is PHI?

The Privacy Rule protects "protected health information" (PHI) from unauthorized uses or disclosures, and it is defined as "individually identifiable health information" (IIHI) that is (1) transmitted by electronic media, (2) maintained in any medium described in the definition of electronic media (the Transactions and Code Sets Rule], or (3) transmitted or maintained in any other form or medium.

According to 45 C.F.R. § 162.103, "electronic media" means the mode of electronic transmission. It includes the Internet (wide open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk or compact disk media.

This definition of PHI clearly subjects most individually identifiable health information to its requirements, whether the information is in electronic, paper or oral form. However, PHI specifically excludes any IIHI in:

- Education records covered by the Family Educational Right and Privacy Act (FERPA);
- Records described at 20 U.S.C. § 1232g(a)(4)(B)(iv) as "records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice"; and
- Employment records held by a covered entity in its role as employer.

To comprehend fully what information is covered as PHI, it is necessary to understand what types of information the Privacy Rule considers IIHI. By definition in 45 C.F.R. § 164.501, "individually identifiable health information" is information that is a subset of health information, including demographic information collected from an individual, that is (1) created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

In addition, 45 C.F.R. § 160.103 provides that "health information" means any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Once the analysis as to whether a health care entity is, in fact, a covered entity has been conducted and the determination as to whether the covered entity uses or discloses PHI has been made, a covered entity can move forward into an analysis of the core elements of the Privacy Rule.

Careful planning and Privacy Rule implementation efforts are critical for all covered entities so that they are in compliance with the Privacy Rule on or before April 14, 2003.

CORE ELEMENTS OF PRIVACY RULE

A. Permitted Uses and Disclosures of PHI

This section contains a sampling of the various uses and disclosures of PHI that are generally permitted under the Privacy Rule, but not each and every one. For the most part, the permitted uses and disclosures outlined below are the embodiment of common sense privacy principles already being followed in most states by most health care entities. These uses and disclosures are, as part of the Privacy Rule framework, technically considered exceptions to the general rule that a covered entity may not use or disclose PHI.

1. Disclosure to Individual

A covered entity may disclose protected health information to the individual who is the subject of the information.

2. Disclosures for Treatment, Payment and Health Care Operations

"Health care operations" include: quality assessment and improvement activities, conducting training programs, case management and care coordination, discussion of treatment alternatives, credentialing or review of health care providers, business, accreditation and licensing, underwriting and premium rating, legal services, auditing, fraud and abuse compliance, case management and planning-related analysis, customer service, internal grievance resolution, sale/transfer/merger of covered entities and due diligence, de-identification of PHI, and fundraising.

A covered entity may use or disclose PHI

- for its own treatment, payment or health care operations (TPO);
- for the treatment activities of a health care provider;
- to another covered entity or health care provider for the payment activities of the entity that receives the information;
- to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is (1) for certain quality assessment and improvement activities or for credentialing or CPE purposes or (2) for the purpose of health care fraud and abuse detection or compliance.

A covered entity that participates in an "organized health care arrangement" may disclose PHI about an individual without the individual's authorization to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

3. Use and Disclosure after Authorization

There are a number of circumstances, found at 45 C.F.R. § 164.508, in which a covered entity must acquire an authorization from the individual *before* it may use or disclose PHI. Primarily, authorizations are required for the following uses or disclosures.

(a) Psychotherapy Notes

"Psychotherapy notes" means "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record." The term excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

"Psychotherapy notes," as defined in the Privacy Rule, does not include the entire mental health record and is therefore less

restrictive than many states' laws with respect to the protections afforded mental health records. As a result, state law that is more restrictive—that is, "more stringent"—than the Privacy Rule's requirements will control the use and disclosure of such information, rather than the Privacy Rule.

(b) Marketing

"Marketing" is a defined term under the Privacy Rule and does not include health-related communications from providers to individuals for which providers receive payment from a third party—for example, a drug manufacturer. Rather, "marketing" is narrowly defined to include only those non-health related communications for which a health care provider receives payment. If the effort does not constitute "marketing," then the mandatory requirement for obtaining an authorization does not apply.

In addition, two activities that fall within the definition of "marketing" are exempted from the mandatory requirement for obtaining an authorization: (1) a face-to-face communication made by a covered entity to an individual and (2) a promotional gift of nominal value provided by the covered entity. If the "marketing" involves direct or indirect payment to the covered entity from a third party—for example, drug manufacturer—the authorization must state that such a payment is involved.

4. Facility Patient Directories and Disclosures to Relatives and Friends

This exception, stated in 45 C.F.R. § 164.510, enables health care facilities to maintain directories of patients under their care and release information about the patient to the public. The information permitted to be used and disclosed is restricted to the individual's (1) name, (2) location in the covered health care provider's facility, (3) condition described in general terms that do not communicate specific medical information about the individual (for instance, "fair," "poor," "stable"), and (4) religious affiliation.

In addition, the information contained in the directory may be disclosed only to members of the clergy or, except for religious affiliation, to other persons who ask for the individual by name. This exception also permits a covered entity to disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI "directly relevant to such person's involvement with the individual's care or payment related to the individual's health care." In both instances, the covered entity must provide the individual with the opportunity to object to the disclosure. (There are some exceptions to this requirement set out in the Privacy Rule, which are not mentioned here.)

5. Potpourri of Uses and Disclosures

(a) Required by Law

45 C.F.R. § 164.512(a), (c), (e) and (f) cover a number of situations.

(i) Domestic Violence

In order to disclose information regarding the victims of domestic violence, the disclosure either must be required by law or the individual must agree to the disclosure, or, if the disclosure is required by law, the individual must be informed of the disclosure. (There are exceptions to the notification/agreement requirement.)

(ii) Court Orders

Situations in which a court order or other legal document with the force of law has been obtained, there is no need to notify individuals of the disclosure or obtain their agreement. However, covered entities must be careful to disclose only the PHI required by the order and no more. Disclosures beyond that ordered to be disclosed would be considered to be in violation of the Privacy Rule.

(iii) Other Requests

Subpoenas, discovery requests, etc. that are not accompanied by a court order are permitted, under certain circumstances. For

example, the covered entity (or business associate disclosing the information on behalf of the covered entity) must obtain satisfactory assurances from the party seeking the PHI that the party either has made reasonable efforts to notify the individual of the subpoena or request or has made reasonable efforts to secure a qualified protective order. (There are additional requirements set out in the Privacy Rule, but these are the primary ones.)

(iv) Law Enforcement

Different types of requests from law enforcement officials authorize different levels of disclosure. Different types of requests from law enforcement officials also may require the agreement of the affected individual.

(b) Public Health Activities

Reports for preventing or controlling disease, injury or disability, including the reporting of disease, injury, vital events (birth or death), and the conduct of public health surveillance, investigations, and similar activities are permitted disclosures under the Privacy Rule. No notice to the individual or approval by the individual is required.

Reports of child abuse or neglect also are permitted, again with no attendant notice or approval requirements.

Reports to a person subject to the jurisdiction of the Food and Drug Administration with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of the product or activity, are permitted. Such purposes include (1) reporting adverse events, (2) tracking FDA-regulated products, (3) enabling product recalls, repairs, etc. or (3) conducting post-marketing surveillance. These disclosures do not require the notice or approval of the individual.

Communicable disease reports are permitted without any notice or approval requirement.

Disclosure to an employer is permitted, but only under very limited circumstances, which are: (1) The health care provider disclosing the employee's information is a member of the employer's workforce who provides health care to the employee concerning the conduct of workplace medical surveillance or the existence of a work-related injury. (2) The employer needs the findings to comply with applicable law. (3) The employer must inform employees of the fact that the information will be disclosed, either by providing a copy of the notice to the employee at the time the health care is provided or by posting the notice.

(c) Disclosures to Health Oversight Agencies

(d) Disclosures Concerning Decedents

(e) Disclosures Concerning Crimes on Covered Entities' Premises.

(f) Disclosures to Organ Procurement Organizations to Facilitate Organ Donations

No notice to or agreement by the individual is required.

(g) Disclosures for Research Purposes

Certain research activities do not require an authorization, or the authorization is waived. The most common circumstance occurs when an institutional review board determines that a waiver is permissible and does so in accordance with certain criteria.

(h) Disclosures to Avert Serious Threat to Health or Safety

(i) Disclosures for Specialized Government Functions

These are military and veteran activities; national security and intelligence activities; protective services for the President and others; medical suitability determinations; correctional institutions; government pro-

grams providing public benefits; and workers' *compensation.*

6. Uses of Limited Data Sets; Fundraising

These exceptions are covered by 45 C.F.R. § 164.514(e)-(g).

Limited data sets may be disclosed for research, public health or health care operations. A data use agreement with the recipient of the limited data set is required.

Fundraising, too, is a limited exception. If the covered entity satisfies the exception, then no authorization is required. (1) The covered entity may use (or disclose to a business associate) demographic information relating to an individual and dates of health care provided to the individual for the purpose of raising funds for the covered entity's own benefit. (2) The covered entity must include in its notice of privacy practices (NPP) that it may use this data for fundraising purposes. (3) The fundraising materials must tell the individual how he or she can opt-out of receiving further fundraising materials. (4) If an individual opts out, the covered entity must make "reasonable efforts" to ensure that future fundraising materials are not sent to the individual.

7. Disclosures to Business Associates

These disclosures are discussed in-depth in the Business Associates section of this article.

B. Authorizations

1. Requirements

An authorization is a document designed to sanction a covered entity's use of specifically identified PHI for a specified purpose, which is other than (1) treatment, payment or health care operations (TPO), or (2) any other use for which disclosure is allowed without an authorization.

There are special rules for authorizations required with respect to psychotherapy notes, as discussed above. The Privacy Rule requires providers to obtain authorization and not use or disclose PHI maintained in psychotherapy notes except for the following uses and/or disclosures: (1) use by the originator of the notes for treatment, (2) use by the covered entity for its own training programs, (3) use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual, (4) use or disclosure when demanded by HHS as part of its enforcement activities, or (5) use or disclosure permitted by Section 164.512(a) (disclosures required by law), Section 164.512(d) (health oversight activities involving the originator of the notes), Section 164.512(g)(1) (disclosures about decedents made to coroners and medical examiners), or Section 164.512(j)(1) (disclosures a covered entity is permitted to make to avert a serious threat to health or safety).

2. Contents

(a) Core Elements

Under 45 C.F.R. § 164.508(c)(1), authorizations must contain certain "core elements." These are:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

2. The name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure.

3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, in-

cluding for the creation and maintenance of a research database or research repository.

6. Signature of the individual and date. If a personal representative of the individual signs the authorization, a description of the representative's authority to act for the individual must also be provided.

(b) Required Statements

In addition to the core elements, Section 164.508(c)(2) provides that the authorization must contain statements adequate to place the individual on notice of all of the following:

1. The individual's right to revoke the authorization in writing, and either (a) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (b) to the extent that the information is included in the notice of privacy practices (discussed below), a reference to the covered entity's notice.

2. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either (a) that the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or (b) the consequences to the individual of a refusal to sign the authorization when the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain the authorization.

3. The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected.

(c) Plain Language

Section 164.508(c)(3) requires that the authorization must be in plain language.

3. Copy

If a covered entity seeks an authorization from an individual, Section 164.508(c)(4) requires that the entity must provide the individual with a copy of the signed authorization.

4. Revocation

An individual may revoke an authorization to a health care provider or other covered entity at any time, provided that the revocation is in writing, but except to the extent that (1) the covered entity has taken action in reliance on the authorization; or (2) if the authorization was given as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself. As a result, a health care provider that wishes to use or disclose PHI pursuant to an authorization and does so after obtaining an authorization from the individual may rely on the authorization, even if the individual immediately revokes it after the service has been provided.

C. Notice of Privacy Practices

Details concerning the contents and dissemination of the notice of privacy practices (NPP) are found at 45 C.F.R. § 164.520.

1. Required Contents

This header must be prominently displayed at the top of the NPP: THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The NPP must contain s description "including at least one example" of the types of uses and disclosures of PHI the covered entity is permitted to make for purposes of "treatment, payment and health care operations." The description "must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required."

There also must be a description of any other purposes for which the covered entity is "permitted or required" to use or disclose PHI without the individual's written authorization in "sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required."

If state or other applicable law prohibits or materially limits any disclosure permitted under the Privacy Rule, that must be

described in the notice.

Every notice must contain a statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke the authorization as provided in the Privacy Rule.

If the covered entity intends to contact the individual for any of the purposes listed below, then the description of the types and uses of disclosures must include a separate statements disclosing that: (1) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual. (2) The covered entity may contact the individual to raise funds for the covered entity. (3) If the covered entity is a group health plan, issues health insurance or serves as a health maintenance organization (HMO) with respect to a group health plan, that the covered entity may disclose protected health information to the employer.

There also must be a statement setting forth and describing the individual's rights to (1) request restrictions on the use and disclosure of PHI, with a statement that the covered entity is not required to agree to such a request; (2) receive "confidential communications" from the covered entity on request, using an alternative address or contact procedure; (3) inspect and copy PHI on request; (4) seek amendment of PHI; (5) receive an accounting of all disclosures made of PHI for which accountings are required under Section 164.528; and (6) if the notice is provided electronically, to receive a paper copy.

The NPP also must include:

- Statements that the covered entity is required by law to "maintain the privacy" of PHI and to provide notice of this legal duty and its privacy practices.
- A statement that the covered entity is required to abide by the terms of its NPP currently in effect.
- A statement that the covered entity reserves the right to change the terms of its NPP, including a description of how it will give individuals notice of such revisions.
- A statement that individuals may complain to DHHS if they believe their privacy rights have been violated by the covered entity, and a brief description of the covered entity's privacy complaint filing processes along with a statement that the individual will not be retaliated against for filing a complaint.
- Contact information for a person or office that can receive complaints and provide further information about the covered entity's privacy practices.
- An effective date for the NPP.

2. Distribution of NPPs

Health plans must distribute their notices of privacy practices no later than the compliance date for the health plan, which is either April 14, 2003, or April 14, 2004, to individuals then covered by the plan. Small health plans: April 14, 2004. A small health plan is one with annual receipts of $5 million or less. All other health plans: April 14, 2003. Thereafter, NPPs must be distributed to new enrollees at the time of enrollment.

Within 60 days of a material revision, the revised NPP must be distributed to then-covered enrollees. At least once every three years, the health plan must notify enrollees of the availability of the NPP and how to obtain it. Health plans can satisfy the distribution requirement by providing one copy of the notice to the enrollee; separate copies do not have to be distributed to covered spouses and dependents.

3. Direct Treatment Relationships

It is important to note the magic words: health care providers "with a direct treatment relationship with an individual." They are the ones who must distribute a NPP to that individual. If there is no direct treatment relationship, there is no notice requirement. So the analysis turns on what constitutes a "direct treatment relationship."

Under Section 164.501 of the Privacy Rule, a "direct treatment relationship" is defined as a treatment relationship between an individual and a health care provider

that is not an "indirect treatment relationship." An "indirect treatment relationship" means a relationship between an individual and a health care provider in which (1) the health care provider delivers health care to the individual based on the orders of another health care provider, and (2) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

There also are rules for how and when these health care providers must provide the NPP. These are:

(1) Provide the notice no later than the date of the first service delivery or, in an emergency situation, as soon as reasonably practicable after the emergency treatment situation.

(2) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment or receipt of the notice, and if that is not obtained, document the good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.

(3) Providers that "maintain a physical service delivery site" must both post the notice "in a clear and prominent location where it is reasonable to expect individuals . . . to be able to read the notice" and make copies available for individuals to take with them.

(4) A covered entity that maintains a website describing its services or benefits must "prominently" post its NPP there and "make the notice available electronically through the website."

(5) NPPs may also be provided by e-mail, subject to prior agreement by the individual.

(6) Health care providers that are part of an organized health care delivery arrangement may use a joint NPP.

D. Minimum Necessary Rule

The Privacy Rule is centered on the concept that, when using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request. In other words, even if a use or disclosure of PHI is permitted, covered entities must make reasonable efforts to disclose only the minimum amount of information necessary to achieve the purpose for which it is being used or disclosed.

1. Uses of PHI

Under 45 C.F.R. § 164.514(d)(2)), a covered entity must identify (1) those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (2) for each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access. In doing so, a covered entity must make reasonable efforts to limit the access to such persons or classes of persons to PHI, consistent with the category or categories identified.

2. Disclosures of PHI

Under 45 C.F.R. § 164.514(d)(3), for any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, a covered entity must (1) develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and (2) review requests for disclosure on an individual basis in accordance with such criteria.

A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as being the minimum necessary for the stated purpose when (1) making disclosures to public officials permitted under the Privacy Rule, if the public official represents that the information requested is the minimum neces-

sary for the stated purpose(s); (2) the information is requested by another covered entity; (3) the information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or (4) documentation or representations that comply with the applicable requirements have been provided by a person requesting the information for research purposes.

3. Requests for PHI

Under 45 C.F.R. § 164.514(d)(4), a covered entity must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities. For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

For all other requests, a covered entity must (1) develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made; and (2) review requests for disclosure on an individual basis in accordance with such criteria.

4. Special Content Requirement

45 C.F.R. § 164.514(d)(5) is an important aspect of the minimum necessary rule, and it likely will require most covered entities and business associates to modify their current behavior with respect to the use, disclosure and requesting of medical records. It states that for all uses, disclosures or requests to which the requirements of the minimum necessary rule apply, a covered entity may not use, disclose or request an entire medical record, *except* when the entire record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

To put it another way, covered entities should not use, disclose or request an entire medical records unless it is really needed.

5. Six Exceptions

As with most requirements of the Privacy Rule, there are exceptions to the minimum necessary rule. When one of the following situations arises, covered entities and their business associates need not follow the rule:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual or in response to a request that the Privacy Rule allows an individual to make (Sections 164.524 and 164.528);
- Uses or disclosures made pursuant to an authorization under Section 164.508;
- Disclosures made to to Health and Human Services in response to it's authority to enforce HIPAA's privacy protections. HHS authority appears in Sections 160.300-160.312, Part 160, Subpart C;
- Uses or disclosures that are required by law, as described by Section 164.512(a); and
- Uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

The business associate provisions of the Privacy Rule pseudo-regulate third-party businesses (that is, non-covered entities) who receive PHI from a covered entity by imposing additional obligations on covered entities with respect to the PHI shared with those with whom it does business. Because a covered entity is bound by the privacy standards of the Privacy Rule, HHS deemed it necessary to safeguard information transmitted from a covered entity to a third party that is performing a function for or on behalf of that covered entity. Otherwise, a covered entity could contractually

avoid complying with the Privacy Rule by transferring certain responsibilities to others.

A. Who Is Business Associate

Simply stated, a business associate is an entity that uses, discloses, creates or obtains PHI in performing a function, activity or service on behalf of a covered entity. The key to understanding the business associate provisions is understanding that not all third parties doing business with covered entities are considered business associates under the Privacy Rule. It is only those entities that act "on behalf of" a covered entity that fall within the ambit of the business associate rules.

Specifically, "business associate" means, with respect to a covered entity, one who:

> (a) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
>
> (1) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
>
> (2) Any other function or activity regulated by this subchapter; or
>
> (b) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

A covered entity participating in an organized health care arrangement that performs a function or activity as described above to, for or on behalf of such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in the organized health care arrangement. However, a covered entity may be a business associate of another covered entity.

Certain individuals or entities that would appear to be business associates actually are not considered business associates under the Privacy Rule. The following are excepted from the business associate requirements: (1) a covered entity's workforce, (2) a physician or contractor of a covered entity, (3) government-sponsored programs, (4) affiliated organizations deemed a single-covered entity, and (5) a health plan that receives PHI solely for payments purposes.

A covered entity may disclose PHI to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. This standard does not apply (1) with respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual; (2) with respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the applicable requirements of the Privacy Rule apply and are met; or (3) with respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for

the performance of such functions by the health plan and the agency other than the agency administering the health plan.

A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications and requirements of the business associate provisions. A covered entity must document the satisfactory assurances required by this Privacy Rule through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements.

B. Business Associate Agreements

1. When Required

Covered entities must have agreements with all their business associates in order to disclose PHI to the business associate. The agreement must be done in advance of any disclosure of PHI and must contain the satisfactory assurances mentioned above. An agreement with a business associate is a written assurance outlining responsibilities, and it is required when:

(1) The covered entity is disclosing PHI to someone or some organization that will use the information on behalf of the covered entity.

(2) The business associate will be creating or obtaining PHI on behalf of the covered entity.

(3) The business associate is providing services to or for the covered entity and the provision of those services involves disclosure of PHI.

Under certain circumstances, a business associate agreement is not required: (1) when a covered entity discloses PHI to a health care provider concerning treatment of the individual; (2) for the provision, coordination or management of health care and related services, including the coordination or management of health care by a health care provider with a third party; (3) where the disclosure is a consultation between health care providers related to a patient; and (4) in situations involving the referral of a patient for health care from one provider to another.

2. Model Provisions

The final Privacy Rule contains what are called "Model Business Associate Contract Provisions," which are available at aspe.os.dhhs.gov/admnsimp and which will alleviate some of the burden associated with complying with this portion of the rule. In a nutshell, a business associate agreement must contain the following 12 elements:

(1) It must specify the permitted and required uses and disclosures of PHI by the business associate.

(2) It may permit the business associate to use and disclose PHI for its management and administration.

(3) It may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(4) It may not authorize the business associate to use or further disclose the information in any manner that would violate HIPAA regulations or the contract.

(5) It must require the business associate to employ appropriate safeguards to prevent the use or disclosure of PHI, other than as provided for by the agreement.

(6) It must require the business associate to report to the covered entity any use or disclosure of PHI not authorized by the agreement.

(7) It must require the business associate to hold its employees, agents and subcontractors to the same standards as the business associate.

(8) It must require the business associate to make PHI available to the covered entity when requested.

(9) It must require the business associate to make PHI available for the covered entity to amend the PHI and provide accounting of disclosures.

(10) It must require the business associate to maintain records for HHS inspection.

(11) It must permit the covered entity to terminate the agreement if covered entity determines that the business associate has materially breached the agreement.

(12) It must require that when the agree-

ment terminates, the business associate will return or destroy all PHI in its possession, including any copies. If it is not feasible or practicable to destroy a to do so, the agreement must specify that the contract's protections will continue as long as PHI is in business associate's possession.

3. Issues to Consider

Some issues, but certainly not all, that should be addressed and considered by the covered entity when drafting its business associate agreements are (1) audit and inspection rights; (2) identification of the custodian(s) of the designated record set; (3) safeguarding the information contained in the designated record set; (4) determining who is in the best position to understand and apply state legal standards to health information that is subject to special legal protection (for example, HIV, mental health, and/or drug or alcohol treatment records); (5) deciding which party will pay for the maintenance of the designated record set; (6) identifying agreements that the business associate has with its subcontractors and agents; and (7) if the business associate retains the PHI after the termination of the contract, determining whether the parties' indemnification clauses survive if the business associate improperly discloses PHI.

It is important for covered entities to recognize that they may well be held to have violated the business associate provisions of the Privacy Rule if they knew of pattern of activity of a business associate that might constitute a material breach of the parties' contract, unless the covered entity takes reasonable steps to cure the breach, and, if the cure is unsuccessful, the covered entity terminated the contract or reported the breach to HHS.

Fortunately, the covered entity is not obligated to monitor the business associate, but it does have a duty to mitigate, to the extent practicable, any harmful effect known to the covered entity to arise from inappropriate disclosure of PHI by a business associate. Thus, oversight or due diligence may be appropriate, depending on the nature of the relationship with the business associate and the sensitivity of the PHI being used and disclosed.

4. Compliance Dates

Requests were made by various sectors of the health care industry to extend the Privacy Rule compliance dates because covered entities were finding it difficult, if not nearly impossible, to complete everything required by April 14, 2003. No extension was granted, but under the final rule they were granted a one-year reprieve from the business associate provisions, until April 14, 2004, under certain circumstances.

Covered entities were given an extension for incorporating the business associate agreement provisions into current contracts that do not come up for renewal before April 14, 2003. On those contracts, covered entities have until either the renewal date of the contract or April 14, 2004, whichever is later. In other words, covered entities cannot enter into new arrangements without incorporating business associate language, but they have an additional year from the original compliance date to bring existing contracts into compliance.

SOME ADDITIONAL TECHNICAL IMPLEMENTATION REQUIREMENTS

A. Individuals' Rights

1. Right to Inspect, Copy, Access

Under the Privacy Rule, individuals have the right to inspect or copy their PHI contained in a "designated record set" for as long as the PHI is maintained in that set. As with most of the Privacy Rule's mandates, there are exceptions to this basic rule. There is no right to inspect and copy (1) psychotherapy notes; (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and (3) PHI subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. § 263a, to the extent the provision of ac-

cess to the individual would be prohibited by law.

Moreover, the right to access or to appeal a denial of access is not required to be given an individual in the following circumstances:

- A covered entity that is a correctional institution or acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining the copy would jeopardize the health, safety, security, custody or rehabilitation of the individual or of other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for the transporting of the inmate.
- An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
- An individual's access to protected health information contained in records subject to the Privacy Act, 5 U.S.C. § 552a, may be denied *if* the denial would meet the requirements of that act.
- An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality *and* the access requested would be reasonably likely to reveal the source of the information.

In addition to these situations, there are still other circumstances under which the right to access is not required, but an individual is entitled to appeal that determination. Under these exceptions to the general rule providing a right to access, covered entities must have appeals procedures in place that comply with certain requirements set out in the Privacy Rule.

Access can be denied, but an appeal must be permitted, when in these three situations:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- The protected health information makes reference to another person, unless the other person is a health care provider, and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

Under the Privacy Rule, written denials must be provided to the individual requesting access and must be provided in a timely fashion. The denial must be in plain language, must describe the basis for the denial, must explain any appeal rights that may exist, and must notify the individual that the individual may complain to the covered entity or to DHHS.

In providing individuals with the right to access their PHI, covered entities and their business associates must provide access only to PHI maintained in a "designated record set," as that term is defined in the Privacy Rule.

"Designated record set" means a group of records maintained by or for a covered entity that is (1) the medical records and billing records about individuals maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the covered entity to make decisions about individuals.

To understand what constitutes the

phrase "group of records," as used in the definition of "designated record set," it is necessary to look to the Privacy Rule definition of "record." This word is said to mean any item, collection or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for a covered entity.

In providing individual access to PHI in the designated record set, covered entities must do the following:

- Provide access to inspect or copy PHI in the designated record set or deny access within 30 days of the receipt of the request.
- If the request for access is for protected health information not maintained or accessible to the covered entity on-site, the covered entity must provide access or deny access no later than 60 days from the receipt of the request.
- The covered entity can extend these time frames once for 30 days. The covered entity must notify the individual of the need and reasons for the extension within the original, required time period.
- Provide access in the form requested by the individual. If that form is not readily reproducible, then provide access in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.
- The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if (a) the individual agrees in advance to receipt of a summary or explanation; and (b) the individual agrees in advance to the fees imposed, if any, by the covered entity for the summary or explanation.
- If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of (a) copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual; (b) postage, when the individual has requested the copy, or the summary or explanation, be mailed; and (c) preparing an explanation or summary of the protected health information, if agreed to by the individual.

2. Right to Request Amendment

Individuals are entitled to request that covered entities amend the PHI contained within the designated record set, but the entities do not have to honor these requests. If the request for amendment is denied, certain procedures set out in the Privacy Rule must be followed. For example, documentation of the request and denial must be added to the designated record set.

In satisfying the requirements of this provision, covered entities must document the title(s) of the person(s) or office(s) responsible for receiving and processing requests for amendments and then retain that documentation. In addition, they must assure a timely response to a request for amendment—60 days for certain requests and 30 days for others. Covered entities also must (1) make sure that accepted amendments will be incorporated in (or linked to) the designated record set, (2) make sure that they inform the individual that the amendment has been accepted, and (3) acquire the individual's agreement to have the covered entity notify the people with whom the amendment needs to be shared.

3. Right to Accounting of Disclosures

The right to an accounting of disclosures is very limited, since most of the disclosures of PHI that are made are exempt from the accounting requirement. (There is a list of exceptions at 45 C.F.R. § 164.528(a)(1)(i)-(viii). If the disclosure is not excepted from the accounting requirement, then the covered entity must account for disclosures for the six-year period preceding the request for an accounting. The individual can designate a shorter period.

The accounting of disclosures must include: (1) the date of the disclosure; (2) the

name of the entity or person who received the PHI and, if known, the address of such person or entity; (3) a brief description of the PHI disclosed; and (4) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis of the disclosure, or, in lieu of such statement, a copy of a written request for disclosure under Sections 164.502(a)(2)(ii) or 164.512, if any. There are additional requirements for multiple disclosures to the same person or entity.

The first accounting of disclosures to an individual in any 12-month period must be provided without charge. Thereafter, a covered entity may impose a "reasonable, cost-based fee" for each subsequent request for an accounting by the same individual within that 12-month period. However, a covered entity may charge the fee only if it has informed the individual of the existence of the fee in advance and provided the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

Covered entities should appoint someone to be responsible for receiving, processing and documenting requests for accountings just as they do for requests for amendment.

B. De-identification

De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. A covered entity may determine that health information is de-identified, and therefore is not IIHI, only if certain, very technical requirements are met.

In the first instance, information may be classified as having been "de-identified" when a person with appropriate knowledge and experience (1) applies generally accepted statistical/scientific principles and methods and determines that the risk is very small that the information could be used to identify an individual and (2) documents the methods and results of the analysis.

Another method of de-identification also may be employed by a covered entity or a business associate acting on behalf of the covered entity. Information is "de-identified" where all of the following identifiers of the individual or of relatives, employers or household members of the individual are removed from the information and the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify the individual: (1) names; (2) all geographic subdivisions smaller than a state (3) all elements of dates (except year) for dates related to the individual: birth date, admission date, discharge date, date of death, all ages over 89 and all elements of date (including year) that are indicative of such age; (4) telephone numbers; (5) fax numbers; (6) e-mail addresses; (7) Social Security numbers; (8) medical record numbers; (9) health plan beneficiary numbers; (10) account numbers; (11) certificate/ license numbers; (12) vehicle identifiers, serial numbers, license plate numbers; (13) device identifiers and serial numbers; (14) URLs; (15) IP address numbers; (16) biometric identifiers, including finger and voiceprints;(17) full face photographic images and any comparable images; (18) any other unique number, characteristic, code.

A covered entity may use PHI to create information that is not IIHI or disclose PHI only to a business associate to do so on its behalf, whether or not the de-identified information is going to be used by the covered entity. Health information that has been de-identified is not considered IIHI, and the requirements of the Privacy Rule do not apply to de-identified information, provided that (1) disclosure of a code or other means of record identification designed to enable the information to be re-identified is disclosure of PHI, and (2) if de-identified information is re-identified, it may be used or disclosed only as PHI is permitted to be used or disclosed under the Privacy Rule.

A code or other means of record identification may be assigned to de-identified information so that it can be re-identified, but

only if (1) the code or other means is not derived from or related to information about the individual and cannot be translated to identify the individual, and (2) the covered entity does not use or disclose the code or mechanism for re-identification.

As a rule of thumb, covered entities may choose simply to assume all information is PHI. For all practical purposes, covered entities probably will receive, use and disclose PHI in the course of their businesses, not de-identified information, except in very limited circumstances, such as researching.

C. Appointment of Privacy Officer

Under Section 164.530 of the Privacy Rule, each covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the covered entity. In addition, each covered entity must designate a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered by the notice of privacy practices.

D. Workforce Training and Education

Covered entities also must train their workforces on the policies and procedures with respect to PHI required by the Privacy Rule, to the extent that training is necessary and appropriate to carry out their functions within the covered entity. There are specific requirements for training set out in 45 C.F.R. § 164.530.

Training must be provided to each member of the workforce by no later than the compliance date for the covered entity. Thereafter, each new member of the workforce must be trained within a reasonable time after the person joins the workforce. If material changes are made to the policies and procedures required by the Privacy Rule, all members of the workforce who are affected by those changes must be trained on the changes within a reasonable time after such changes become effective.

E. Security

Also mandated by Section 164.530, a covered entity must have in place appropriate administrative, technical and physical safeguards—that is, security—to protect the privacy of PHI. Privacy is the individual's right over the use and disclosure of his or her PHI, and it includes the right to determine when, how and to what extent PHI is shared with others. Security, on the other hand, is the specific measures a health care entity must take to protect PHI from any unauthorized breaches of privacy, for instance, if information is stolen or sent to the wrong person in error. Security also includes measures taken to ensure against the loss of integrity of PHI, such as if a patient's records are lost or destroyed by accident. In other words, privacy concerns what information is covered, and security is the mechanism used to protect it.

HIPAA requires "reasonable and appropriate" general security measures, and the Proposed Security Rule prescribes a detailed and comprehensive set of activities to guard against the unauthorized disclosure of PHI stored or transmitted electronically or on paper. The specific requirements set out in the Proposed Security Rule are beyond the scope of this article.

Much confusion has arisen within the health care industry as to exactly what security measures will be required under HIPAA in order for covered entities to be in compliance with the Privacy Rule. This is because privacy and security are addressed in separate regulations with *separate* compliance dates and separate requirements.

The best advice is that covered entities should implement both privacy and security measures to comply with the Privacy Rule deadline of April 14, 2003. Why? First, HIPAA applies to health information and doesn't require the final Security Rule to become effective. It states that each covered entity that

> maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safe-

> guards—(A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such [covered entity].

Second, as discussed above, the Privacy Rule provides that a covered entity *must* have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI. A covered entity *must* reasonably safeguard PHI from any intentional or unintentional use or disclosure in violation of HIPAA. In addition, a covered entity *must* reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Combating threats to both health information security and privacy should be at the heart of each covered entity's Privacy Rule compliance efforts. Security threats include:

- intentional misuse by internal personnel;
- malicious or criminal by from internal personnel;
- unauthorized physical intrusion of data systems by external persons; and
- unauthorized intrusion of data systems by external persons via information networks.

The greatest security threats are not hackers but insiders. Some key areas of security concerns are:

- unprotected Internet;
- web browsing and cookies;
- authentication;
- networks and firewalls;
- lack of physical security;
- hackers and other illegality;
- internal mischief and disgruntled employees; and
- data sharing.

The Proposed Security Rule probably will not be substantially modified when it is issued in its final form. In fact, most of the security components of HIPAA are already being used by other industries, such as retail and banking. Unfortunately, even basic security measures are new to certain sectors of the health care industry, which is generally considered to be 10 to 15 years behind other industries with regard to security. The final Security Rule will mandate safeguards for physical storage, maintenance, transmission and access to PHI. It will apply only to PHI, not to all individually identifiable health information. All covered entities (and by extension, their business associates) will be required to develop and document a security program to guard against real and potential threats of disclosure or loss, which will include policies, procedures and safeguards to protect PHI stored on computer systems and in physical office spaces.

Moreover, the Security Rule will require covered entities to appoint a security officer, just as the Privacy Rule requires the appointment of a privacy officer. Covered entities should recognize that security readiness is not just an information technology project; it involves people and processes, as well as IT. It's not surprising that HIPAA compliance has been identified as the top IT priority now and in the next two years, according to the 13th Annual HIMSS Leadership Survey sponsored by Superior Consulting Co.[4] Covered entities must decide what security measures need to be implemented. They cannot wait until the final Security Rule is published to begin thinking about security issues.

HIPAA PENALTIES AND ENFORCEMENT

The penalty provisions of HIPAA apply to non-compliance by covered entities with any of the requirements of the Administrative Simplification rules. However, the Privacy Rule creates the most HIPAA compliance pitfalls for covered entities.

A. Civil Penalties

Civil fines of $100 per violation up to $25,000 for multiple violations of the same

4. The full report, including graphics, is available at www.himss.org/2002survey/.

standard in any given calendar year may be imposed, but there are many instances in which the civil fines can be lifted or reduced:

(1) If an offense is otherwise punishable (that is, criminally sanctionable) under HIPAA, a civil penalty may not be imposed additionally.

(2) A civil penalty may not be imposed if it is established to the satisfaction of HHS that persons liable for the penalty did not know, and by exercising reasonable diligence would not have known, that they violated the provision.

(3) A civil penalty may not be imposed if the failure to comply was due to reasonable cause, not willful neglect, and the failure is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. The 30-day period may be extended on request for a period of time determined by considering the nature and extent of the failure to comply. If HHS determines that a person failed to comply because the person was unable to comply, it may provide technical assistance to the person during the 30-day period.

(4) In the case of a failure to comply owing to reasonable cause and not to willful neglect, any penalty that is not entirely waived may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

There is no private civil right of action under HIPAA for individuals to bring lawsuits on the basis of a HIPAA violation alone. However, individuals may sue on "invasion of privacy" claims, and they probably will attempt to use the Privacy Rule as a general "standard of care" for patient privacy.

B. Criminal Penalties

Criminal fines can be imposed for knowing violations of HIPAA on a sliding scale based on the egregiousness of the violation: (1) not more than $50,000 and/or not more than one year in prison for knowingly violating HIPAA; (2) not more than $100,000 and/or not more than five years in prison for using false pretenses to violate HIPAA; and (3) not more than $250,000 and/or not more than 10 years in prison for violating HIPAA with the intent to gain personally or commercially or with intent to cause malicious harm by the misuse of IIHI.

There are no exceptions explicitly set out in the HIPAA statute for mitigation or waiver of the criminal penalty provisions.

C. Enforcement

No formal mechanism is in place now for policing covered entities' HIPAA compliance. The HHS Office for Civil Rights has been entrusted with the task of enforcing HIPAA, but it has stated that as long as covered entities' compliance efforts are "reasonable and appropriate," it will work with covered entities to bring them into compliance.

HIPAA PRE-EMPTION

Similar to other federal mandates, HIPAA generally pre-empts conflicting provisions of state laws. The rule stated in 45 C.F.R. § 160.203 is that where the Privacy Rule conflicts with a provision of state law, the Privacy Rule controls.

There are, of course, exceptions to this general rule. The primary exception is where a state law that relates to the privacy of IIHI is "more stringent" than the Privacy Rule. In that instance, state law controls. According to Section 160.202, state law is "more stringent" than the Privacy Rule if:

(1) the state law prohibits or restricts a use or disclosure that that the Privacy Rule would permit, except if the disclosure is (i) required to determine whether a covered entity is in compliance with the Privacy Rule or (ii) to the individual;

(2) the state law permits greater rights of the individual to access or amend IIHI;

(3) the state law provides for giving the individual a greater amount of information about a use, disclosure, right or remedy;

(4) the state law involves the form, sub-

stance or need for giving express legal permission, and the law provides requirements that narrow the scope or duration, increase the privacy protections, or reduce the coercive effect of the circumstances surrounding the express legal permission;

(5) the state law provides for more detailed or longer record-keeping requirements relating to accounting of disclosures; or

(6) the state law generally provides greater privacy protection for the individual.

Second, where a determination is made that state law is necessary to do any of the following, state law controls: (1) prevent fraud and abuse; (2) ensure appropriate state regulation of insurance and health plans; (3) assist with state reporting on health care delivery or costs; or (4) serve a compelling need related to public health, safety, or welfare, with a minimal intrusion on privacy rights.

Third, where a state law is principally designed to regulate the manufacturing, distribution, registration or dispensing or other control of controlled substances, state law controls.

Fourth, where a state law provides for more detailed reporting of disease or injury, child abuse, birth or death or for more specific conduct of public health surveillance, investigation or intervention, state law controls.

Finally, where a state law requires a health plan to report or provide access to information for any of the following purposes, state law controls: (1) management audits, (2) financial audits, (3) program monitoring, (4) program evaluation or (5) licensure or certification of facilities or individuals.

As is evident, the pre-emption analysis is a significant undertaking. All states have comprehensive regulatory, statutory and common law privacy schemes that must be considered by covered entities as part and parcel of their Privacy Rule compliance efforts. This analysis is time consuming and will be different for each covered entity in each state. Where an entity that is responsible for being in compliance with the Privacy Rule in more than one state—or all 50 states, for that matter— by April 14, 2003, the task can seem more than a little overwhelming.

Many states, medical associations and large health care organizations have commissioned task forces to analyze state law with respect to HIPAA pre-emption. For example, the Health Privacy Project, part of the Institute for Health Care Research and Policy at Georgetown University, has conducted a 50-state survey of privacy laws, and the results of its study are available to the general public at no cost. However, these analyses are just the starting point in any pre-emption analysis. The federal government has been asked to provide additional guidance on this aspect of the Privacy Rule in particular. Whether that guidance will be forthcoming remains to be seen.

ADDITIONAL RESOURCES

The following are a few of the many resources available to covered entities for guidance with respect to HIPAA compliance:

- U.S. Department of Health and Human Services: http://aspe.os.dhhs.gov/admnsimp/
- HHS Office for Civil Rights: www.hhs.gov/ocr/hipaa/
- WEDI-SNIP Workgroup for Electronic Interchange Stategic National Implementation Process: http://snip.wedi.org/
- Health Privacy Project: www.healthprivacy.org
- HIPAAdvisory (Phoenix Health Systems): www.hipaadvisory.com/

Covered entities should consult with health care attorneys who understand the intricacies of the HIPAA Administrative Simplification provisions, in conjunction with their own internal efforts to become complaint with HIPAA. There are certain aspects of each rule, and particularly the Privacy Rule, that all but require the advice of counsel—for examples, drafting compliant policies and procedures, notices of privacy practices, authorizations, business associate agreements, and training programs.

Annual Survey of Fidelity and Surety Law, 2002, Part I

This roundup of recent cases covers public and private construction bonds, fidelity and financial institution bonds, and sureties' remedies

By Bettina E. Brownstein, R. Earl Welbaum, Randall I. Marmor and Roger P. Sauer

Edited by Charles W. Linder Jr.

The annual survey of fidelity and surety law is a project of the IADC Fidelity and Surety Committee and is published in two parts. This is Part I of the 2002 survey. Part II will appear in the July 2003 issue of Defense Counsel Journal.

The sections of the survey were prepared as follows:

"Public Construction Bonds," by Bettina Brownstein, a partner in the law firm of the Little Rock firm of Wright, Lindsey & Jennings. This is her first appearance in the fidelity and survey law annual survey. She holds B.A. (1971) and M.A. (1973) degrees from the University of California at Los Angeles and earned her J.D. degree from the University of the Pacific McGeorge School of Law in 1982.

"Private Construction Bonds," by IADC member R. Earl Welbaum of the Miami (Coral Gables) firm of Welbaum, Guernsey, Hingston, Greenleaf & Gregory.

"Fidelity and Financial Institution Bonds," by IADC member Randall I. Marmor of the Chicago firm of Clausen, Miller P.C.

"Sureties' Remedies," by IADC member Roger P. Sauer of the Westfield, New Jersey, firm of Lindabury, McCormick & Estabrook.

The survey acknowledges the assistance of Michael J. Rune II, Andrew C. Demos and Cole S. Kain.

The survey material is edited by IADC member Charles W. Linder Jr. of the Indianapolis firm of Linder & Hollowell.

I. PUBLIC CONSTRUCTION BONDS

A. Bonds under Federal Laws

Performance bond surety on defaulted federal government contract not entitled to contract funds withheld for violations of David-Bacon Act.

Surety that did not give notice of potential bond default did not have claim since government's disbursement of funds not in derogation of contract.

Only performance bond surety that enters into takeover agreement with government can sue in Court of Federal Claims under Contract Disputes Act.

In *Weschester Fire Insurance Co. v. United States*,[1] Weschester was surety for a contractor who defaulted on a contract to rehabilitate the U.S. Coast Guard waterfront facility at Baton's Neck, New York. The contract incorporated the Davis-Bacon Act, 40 U.S.C. § 276a, which requires laborers to be paid no less than rates specified by the U.S. Department of Labor. The act also mandates that these rates be a part of the contract. After the default, the surety claimed entitlement to the entire unpaid contract balance, including $60,216.58 that the government, finding the contractor had violated the act, had earmarked as restitution for wages and fringe benefits to underpaid workers.

The contracting officer disagreed, and Weschester sued to reverse of the contracting officer's decision. Ruling on a motion for summary judgment, the Court of Federal Claims affirmed the decision of the contracting officer, finding the central and controlling fact to be the incorporation of the act in the contract with its provision

1. 52 Fed.Cl. 567 (2002).

that the Coast Guard was to withhold payments to the contractor if any Davis-Bacon violations were committed. Not surprisingly, the court found the workers' rights to the contract funds to be superior to those of the Coast Guard, the contractor and the surety.

Weschester also asserted entitlement to $32,000, the amount of the last progress payment to the contractor, on the ground that at the time it made the payment, the Coast Guard already had decided to terminate the contract. The Coast Guard responded that the surety had failed to give requisite notice of the default and had not requested that further progress payments be withheld. The court agreed, holding that the government, as obligee, owes only an equitable duty to a surety when the latter notifies the former that there has been a default under the bond. In this case, the court found that the government had kept Westchester informed by copying it on cure and show cause notices, thus giving the surety opportunity to give notice of the contractor's potential default on the bonds and to request that future progress payments be withheld. Even so, the court stated that the government had a duty to Westchester, in the absence of valid notice by the surety of a default, if the government's progress payment was not in accordance with the contract provisions. In this instance, the Coast Guard's payment was held to be proper.

The parties asserted that the court had jurisdiction over the matter under the Contract Disputes Act, 41 U.S. C. § 609(a). The court disagreed. Only a performance bond surety that enters into a takeover agreement with the government and thereby establishes privity with it can maintain an action under the act. This had not occurred in this case.

Surety could not avoid liability on payment bond based on unsatisfied "pay when and if paid" clause in settlement agreement.

Weststar Engineering was prime contractor on a federal project to repaint a Navy crane in Bremerton, Washington. In compliance with the Miller Act, Weststar obtained a payment bond from Reliance Opinion Insurance Co. Weststar and a subcontractor, Walton Technology Inc., entered into a settlement agreement providing that Weststar would be obligated to pay Walton for rental equipment only "when and if paid" by the government. Walton then sued Reliance and the contractor for the amount owed.

The Miller Act creates an obligation on the part of a surety to pay workers and materialmen for "sums justly due." Reliance contended that since the Navy had not paid Weststar, there were no "sums justly due" for which Reliance could be liable, since a surety's liability is coextensive with that of its principal.

In *Walton Technologies Inc. v. Weststar Engioeering*,[2] the Ninth Circuit agreed that generally the rules of suretyship apply to Miller Act cases, but it stated that in the context of the act, a court must look beyond the principal's contractual obligations to the act itself to define the surety's liability. Rights provided by the Miller Act will not be delimited by the contract between the contractor and subcontractor, it stated, and thus Walton's right to recovery on the bond accrued 90 days after it completed its work and not "when and if" the government paid Weststar. The court further found that the subcontractor had not clearly and explicitly waived its right to sue under the act.

A sharply critical dissent declared that the majority's holding appeared to "stand the general rule of suretyship law on its head" in not allowing the surety to occupy the shoes of the principal and avail itself of the principal's defenses. It noted that the majority had determined that a Miller Act surety could be liable to a subcontractor even though the principal owed it nothing.

B. State and Local Bonds

1. Procedural

12-year statute of limitations for ac-

2. 290 F.3d 952 (9th Cir. 2002).

tion on performance bond began to run on date of final loan closing.

The owner of a public housing facility constructed pursuant to an October 22, 1982, contract, sued Seaboard Surety Co. over faulty construction on October 16, 1996, The trial court granted Seaboard summary judgment on the ground that the claim was barred by Maryland's 12-year statute of limitations for actions on bonds.

The court first disregarded, as against public policy, the bond's two-year limitations period in favor of the Maryland statute, but it looked to that bond provision to determine the parties' intent as to when the accrual time commenced and found it to be the date on which the final payment under the contract fell due. This date was October 10, 1984, it concluded, when the state's Community Development Administration requested final payment from the Maryland Housing Fund and stated its belief that the money from the fund was now "payable." Since the contractor had filed suit after October 10, 1996, its claim was time-barred.

This decision was affirmed in *Hagerstown Elderly Associates Limited Partnership v. Hagerstown Elderly Building Associates Limited Partnership* by the Maryland Court of Appeals.[3] The court agreed that the 12-year period applied, but disagreed that this limitation barred the action against the surety. Instead, the appellate court held that, pursuant to the terms of the building contract, the accrual period commenced November 1, 1984, the date of the final loan closing. Embarking on a definitional exploration of the word "payable," it concluded the word meant a sum "that is to be paid" and not that final payment was due.

2. Substantive

Surety liable for defaulting subcontractor's unpaid employment taxes to federal and state governments as intended beneficiaries on bond.

In a 2-1 decision with a strongly worded dissent, a panel of the Ninth Circuit, having considered conflicting precedent and relying on the plain language of a subcontract, found the United States and Hawaii to be intended third-party beneficiaries of a subcontractor's bond. As a result, the subcontractor's surety was obligated to pay Hawaii and the U.S. federal government the defaulting subcontractor's employment taxes. *Island Insurance Co. v. Hawaiian Foliage & Landscape Inc.*[4]

Oahu Construction Co. had contracted with the City and County of Oahu to build a golf course. Oahu subcontracted landscaping work to Hawaiian Foliage & Landscape, which obtained a performance/payment bond from Island Insurance Co. Hawaiian defaulted. Island refused to pay its principal's tax debts. The federal district court granted the surety's motion for summary judgment. 2000 U.S.Dist. Lexis 16749 (D. Haw.).

The Ninth Circuit reversed, applying Hawaiian law and adopting the argument that the terms of the subcontract required Hawaiian to pay all taxes. The bond, in turn, covered its principal's complete performance of the subcontract, which included payment of taxes. Having determined the extent of the surety's duty, the court easily found that the federal and state governments were intended third-party beneficiaries of the bond.

It did so by applying Section 302(1) of the Restatement (Second) of Contracts, which provides that an entity is an intended beneficiary if the "performance of the promise will satisfy an obligation to the promisee to pay money to the beneficiary." Island, the promisor, had promised to ensure Hawaiian's performance, including payment of taxes. This made the governments intended beneficiaries who could bring a direct action against Island.

Island contended that it should not be liable because its intended beneficiary was Oahu, and Oahu could not be responsible for the taxes. The court gave this argument short shrift, instead emphasizing that the language of the subcontract controlled in that it reflected the parties' intention to

3. 793 A.2d 579 (Md. 2002).
4. 288 F.3d 1161 (9th Cir. 2002).

make the bond responsible for the subcontractor's tax liabilities.

Characterizing the majority's decision as "inequitable and unusual" and describing a contract "into which no reasonable man or woman would likely enter," the dissent found, adopting a "reasonable, probable, and natural interpretation" of the contract terms, that the language did not evince an intention that Island be responsible for the taxes. The dissent also contended that the purpose of the bond was to protect the contractor (who had no liability for the unpaid taxes) from Hawaiian's failure to perform and not to protect the federal or Hawaiian governments.

Surety's tender of substitute contractor with new surety did not satisfy surety's obligation to school board.

In *School Board of Broward County, Florida v. Great American Insurance Co.*,[5] the school board appealed a decision granting summary judgment against it in favor of Great American, the surety.

Rockland Construction Co. contracted with the school board to build a high school athletic field and sports complex. Great

American issued a performance bond. Before beginning work, Rockland defaulted, and the board demanded that the surety complete construction. Great American made arrangements for another contractor to do so and to have a new surety guarantee completion. Great American would then be released from its bond. The board rejected this offer and insisted that Great American either serve as general contractor or supervise the new contractor's work.

After negotiations, the board declared the surety in default and sued, arguing that the tender of a substitute contractor and demand for release did not fulfill its obligation to "correct" Rockland's default. The trial court found in favor of the surety.

In a puzzling decision, the Florida Court of Appeal reversed, declaring that to allow Great American to substitute a new contractor would narrow the scope of bond coverage and cause the board to give up its right to insist on performance by the surety. It held that tender of a new contractor and surety was not correction of the contractor's default in that it did not constitute full performance as required by the bond. However, the court did not explain why a new contractor (one that had previously bid on the project) and surety would not constitute full performance, since the end result—a completed athletic facility guaranteed by a surety—would be the same.

Employee leasing contractor could bring suit on general contractor's bond even though contract violated state employee leasing act.

Eastland Financial Services entered into a contract to furnish labor to a general contractor, MC Builders, with Mid-Continent Casualty Co. as surety for MC Builders. At the time of the contract, in violation of New Mexico's Employee Leasing Act, Eastland was not a registered company and had failed to post its own surety bond.

In *Eastland Financial Services v. Mendoza*,[6] the New Mexico Court of Appeals, while conceding that generally a contract made in violation of a statute prescribing penalties is void, looked to the policy of the law violated, the type of illegality involved in the contract and the facts of the case before deciding that the contract was enforceable against the surety on its bond.

Mid-Continent had argued unsuccessfully to the trial court that Eastland should be precluded from bringing suit. The appellate court agreed with the lower court, finding that the factual context and public policy did not favor voiding the contract but instead favored protecting the leased employees.

Factual dispute concerning contractor's substantial compliance with registration statute precluded summary judgment for surety

---

5. 807 So.2d 750 (Fla.App. 2002), *rehearing denied*, March 15, 2002..

6. 43 P.3d 375 (N.M.App. 2002), *corrected* April 8, 2002.

An Alaska trial court dismissed a subcontractor's Little Miller Act claim against the general contractor's surety because the contractor had failed to comply with an Alaska statute that bars a contractor from suing for compensation unless it either met or was in substantial compliance with the statute's registration requirements when the contract was entered into. In *McCormick v. Reliance Insurance Co.*,[7] the Alaska Supreme Court, finding questions of material fact as to whether the contractor had substantially complied with the statute, reversed.

John McCormick orally contracted with Alaska Electric Co., an electrical subcontractor on an Anchorage International Airport runway project, to provide trucking services. The general contractor, Wilder Construction Co., refused payment, claiming that McCormick's work was outside the scope of the agreement to provide end-dump trucking services. McCormick then sued Wilder and its surety, Reliance. Moving for summary judgment, Reliance asserted that McCormick's contractor registration had expired before he contracted with Alaska Electric and that thus his action was barred.

The Alaska Supreme Court discussed the courts' approach to the statute as one of requiring substantial rather than strict compliance in that substantial compliance "affords the public the same protection that strict compliance would offer." Because the court found that the evidence of McCormick's prior registration with the Alaska Division of Occupational Licensing, his valid contractor's license issued by the Municipality of Anchorage, and his state business license, as well as evidence that his bond and insurance had remained in effect after his license had elapsed, raised a factual issue about substantial compliance that warranted reversal of the trial court's dismissal of his complaint.

7. 46 P.3d 1009 (Alaska 2002).

8. 559 S.E.2d 429 (Ga. 2002), *reconsideration denied*, February 25, 2002, *rev'g* 543 S.E.2d 102 (Ga.App. 2000).

II. PRIVATE CONSTRUCTION BONDS

A. Liability of Surety

Under Georgia law, filing of lien-release bond does not create new cause of action for subcontractor against owner. Rather, subcontractor or supplier must first perfect its lien and seek recovery from contractor prior to seeking recovery from owner's surety.

In *Few v. Capitol Materials Inc.*,[8] a property owner, Joseph Few, contracted with the Perez Group, the contractor, to build a house. Six days after filing for bankruptcy, the contractor purchased dry wall materials from Capital Materials, for which it failed to pay, and Capital Materials filed a materialman's lien against Few's property. He discharged the lien by filing a lien-release bond, as provided for in Georgia's mechanic's lien statute, Section 44-14-364 of the Georgia Code. Capital Materials then proceeded directly against Few on the bond without commencing any action against Perez Group. The trial court granted summary judgment in favor of the supplier on its claim, which the Georgia Court of Appeals affirmed.

The Georgia Supreme Court reversed, holding that an owner's filing of a lien-release bond under the Georgia statute does not create a new cause of action for a lien claimant. The bond merely stands in the place of the real property as security for the lien claimant and does not hinder the principal and surety on the bond from raising any defense that would have been available as a defense to the lien foreclosure. The court ruled that a lien claimant must first seek to recover from the contract, with whom it was in privity, and not the owner of the property.

The case was reversed because Capital Materials failed to commence a timely action against contractor before proceeding against Few on his bond or to fall within any of the exceptions of the in the statute.

B. Miscellaneous

Motion to recover attorneys' fees in

action in Florida must be filed within 30 days after filing of judgment, thus surety's claim filed 47 after favorable judgment was untimely.

In *Ulico Casualty Co. v. Roger Kennedy Construction Inc.*,[9] the trial court entered a final judgment in favor of the Ulico Casualty Co., the surety, and its principal under its bond against the general contractor on January 17, 2001. Ulico moved for attorneys' fees 47 days later, on March 6. The trial court held that the motion was untimely under a recent amendments to the Florida Rules of Civil Procedure.[10]

The Florida Court of Appeal affirmed and held that the surety's motion was untimely. Prior to the January 1, 2001, amendment of Rule 1.525, the court explained, an attorneys' fees motion could be filed within a "reasonable time" after entry of the final judgment. It held that in revising Rule 1.525 to specifically state that motions "shall" be served within 30 days after the filing of a judgment and considering the committee note to the rule, which explains that the rule is intended to establish a time requirement to serve for costs and attorneys' fees, the Florida Supreme Court clearly intended to abrogate the long standing "reasonable time" standard.

C. Liability of Surety

Liability of surety under labor and material payment bond claim by construction project staffing company is matter of first impression under New York law, and question is certified to New York's highest court.

In *Tri-state Employment Service Inc. v. Mountbatten Surety Co.*,[11] Team Star Contractors entered into an agreement with O'Ahlborg & Sons to perform construction work at a site in Quincy, Massachusetts. Mountbatten Surety Co. issued two labor and material bonds to Team Star as principal and O'Ahlborg as obligee.

Tri-state then entered into an oral agreement with Team Star to provide employee leasing services. Team Star subsequently failed to make payments on outstanding invoices, and Tri-state filed a proof of claim with Mountbatten seeking payment of $1,113,251.90 under one of the labor and material bonds. Tri-state filed suit, and Mountbatten asserted several affirmative defenses, among which was that Tri-state was not, as a matter of law, a proper claimant under the surety bond. On that basis, the district court granted Mountbatten's motion for summary judgment.

The U.S. District Court for the Southern District of New York held that Tri-State was not a proper bond claimant because as a professional employer organization (PEO), it did not provide labor and material as the terms were used in the language of the bond. The court also noted that Tri-State's efforts to characterize itself as a joint employer of the labors on the project to which the bonds applied did not make it a provider of labor and material itself—Tri-state merely served administrative functions, including payroll and human resource services. These, the court concluded, did not meet the bond's definition of labor and materials. 2001 U.S.Dist. Lexis 6279.

The Second Circuit explained that since this was a diversity case, the law of New York applied. It found that Tri-state's PEO status as a claimant under the surety bond was a matter of first impression in New York's jurisprudence. Noting that the PEO industry has developed only recently and is experiencing fast growth, it certified this question to the New York Court of Appeals: "In the circumstances presented, is a PEO, under New York law, a proper claimant under a labor and materials surety bond?"

The court further noted that in general those who can recover on a payment bond are subcontractors or persons supplying labor or materials to subcontractors or general contractors, and that other jurisdictions hold that lenders or creditor cannot be a proper bond claimant.

Tri-state contended that its status is that

9. 821 So.2d 453 (Fla.App. 2002).
10. *See* 773 So.2d 1099 (Fla. 2000).
11. 295 F.3d 256 (2d Cir. 2002).

of an "employer" of the workers involved at the project and that it is treated accordingly under the Internal Revenue Code and other statutes, such as the Fair Labor Standards Act. The Second Circuit observed that California cases have held that the legal status of an employer of laborers furnished to a work of improvement is crucial factor that distinguishes a person who "furnishes" laborers to a project "from a person who merely organizes the work force, performs administrative functions, advances wages, or does all three in behalf of another."

D. Indemnity

Surety asserted valid defense to nonpayment under bond due to subcontractor's failure to execute condition precedent indemnity/hold harmless agreement.

In *Team Land Development Inc. v. Anzac Contractors Inc.*,[12] a subcontract contained a provision that made final payment contingent on the subcontractor (Anzac) providing releases to the prime contractor (Team Land) in "satisfactory" form holding the prime contractor and owner free and harmless from all claims arising from or in connection with the subcontract. Team Land issued a check to the escrow account of Anzac's attorney, but Anzac did not provide the releases as called for in the subcontract.

The trial court construed the release provision of the subcontract as "ambiguous," thereby relieving Anzac from the condition precedent to payment. It granted summary to Anzac.

The Florida Court of Appeal reversed, referring to a dictionary definition of "satisfactory" as meaning "giving satisfaction sufficient to meet a demand or requirement; adequate."

Since a surety is afforded any defenses available to the contractor,[13] the court stated, the surety in this case, USF&G, could assert Anzac's failure to comply with a condition precedent as a defense to nonpayment. Therefore, Anzac's failure to abide by a valid condition precedent excused Team Land and the surety from making payment until such time as Anzac provided the requisite release.

The court went further and held that even if it were to determine that the language used was ambiguous, invalidating the waiver provision was not the correct course of action. The trial court "could have easily interpreted the release provision according to the intent of the parties and the custom of the industry."

III. FIDELITY AND FINANCIAL INSTITUTION BONDS

A. Emloyee Dishonesty

Trade secrets not covered property under crime policy.

In *Holloway Sportswear Inc. v. Transportation Insurance Co.*,[14] Holloway claimed that its former employee stole trade secrets, including clothing designs and pricing information, which he sold to a competitor. It sought recovery of its losses under a policy that included commercial crime coverage. The policy indemnified Holloway for damage to "covered property," which was defined as "money" and "securities" and tangible property other than money and securities.

The federal district court in the Southern District of Ohio entered summary judgment for the insurer, holding that the plaintiff's trade secrets were intangible property and therefore did not fall within the policy's definition of "covered property."

B. Definition of Employee

Provision in policy defining "employee" as person employed by "employment contractor" was ambiguous.

In *Mansion Hills Condominium Ass'n v. American Family Mutual Insurance Co.*,[15] a condominium association claimed that an

12. 811 So.2d 698 (Fla.App. 2002), *rehearing denied*, March 22, 2002.
13. *Citing* C.A. Oakes Constr. Co. v. Ajax Paving Indus. Inc., 652 So.2d 914, 916 (Fla.App. 1995).
14. 177 F.Supp.2d 764 (S.D. Ohio 2001).
15. 62 S.W.3d 633 (Mo.App. 2001).

office manager, who had been furnished by a management company and embezzled funds from the association's checking account, was its employee. It sought recovery under an employee dishonesty endorsement of a property and business insurance policy.

The trial court entered judgment for the insurer, finding that the office manager was not an "employee" within the meaning of the policy, but the Missouri Court of Appeals reversed.

The policy covered acts of dishonesty by an "employee" of the insured, which included any person employed by an "employment contractor" while the person performed services under the insured's direction and control. The association had hired KEM Construction Co. to manage the property, and KEM placed the office manager on site. KEM paid all salary and employment benefits, but the office manager was subject to the direction and control of the association. The insurer maintained that "employment contractor" clearly referred to a temporary insurance agency, and therefore KEM was not an "employment contractor" as that term was used in the policy.

The court concluded that the term was subject to more than one reasonable interpretation, and therefore it was ambiguous and must be construed in favor of the insured.

Question of fact whether person responsible for loss was employee or independent contractor.

In *Mountain Lodge Ass'n v. Crum & Forster Indemnity Co.*,[16] Mountain Lodge, an unincorporated association, hired Norman D. Tyler as a "construction manager" to oversee renovations of its condominium facility. Tyler allegedly overbilled the plaintiff for labor and materials and misappropriated funds, and the plaintiff sought recovery of the loss under a policy that included employee theft coverage. The insurer denied coverage on the ground that Tyler was an independent contractor and not an employee within the meaning of the policy.

The intermediate appellate court agreed and affirmed the grant of summary judgment in favor of the insurer, but the West Virginia Supreme Court of Appeals reversed.

The supreme court observed that the distinction between an employee and an independent contractor is whether an insured has the right to control and supervise the work performed. The trial court had concluded that the plaintiff never exercised control over Tyler, but the court noted that the failure to exercise control did not dictate whether the plaintiff had the right to do so. The court held that there was a genuine issue of material fact whether the plaintiff had the right to supervise and control Tyler's work,

C. Exclusions

Insurance broker who furnished clients to premium finance company was intermediary or finder within meaning of exclusion.

First Insurance Funding Corp. v. Federal Insurance Co.[17] involved construction of an exclusion in a financial institution bond that barred coverage for losses caused by an agent, broker, independent contractor, intermediary, finder or similar representative. First Insurance sought a declaratory judgment that it was entitled to indemnification and that Federal's denial of the claim amounted to an unreasonable and vexatious action under the Illinois Insurance Code. The federal district court held that the exclusion applied to the loss claimed by the plaintiff and dismissed the action. The Seventh Circuit affirmed.

First Insurance was engaged in an insurance premium finance business. Colesons Insurance Group, an independent insurance broker, frequently referred clients to First Insurance to obtain financing for payment of insurance premiums. Colesons assisted clients in preparing the loan application and finance agreement required by First Insurance. In the transaction at issue, First

16. 558 S.E.2d 336 (W.Va. 2001).
17. 284 F.3d 790 (7th Cir. 2002).

Insurance disbursed $4.3 million to Colesons on the faith of forged loan documents and sought recovery of the loss under its financial institution bond,

The Seventh Circuit concluded that Colesons was an intermediary, finder or similar representative of the insured within the unambiguous meaning of the exclusion. The court noted that Colesons's responsibility for bringing businesses together to consummate a transaction was the precise type of conduct in which an intermediary or finder typically engages. It rejected First Insurance's contention that Colesons did not act as its intermediary in the course of fraudulent transactions involving loans to fictitious entities. It held that First Insurance bore the risk of cloaking Colesons with the authority to act as its intermediary.

D. Termination of Coverage

Coverage terminated as to employee when audit first revealed unauthorized expenditures; proof of loss was untimely.

In *Acadia Insurance Co. v. Keiser Industries Inc.*,[18] the president of Keiser, the insured, made unauthorized personal charges on the company credit card. Keiser, a constructor of modular homes, sought recovery of the loss under a policy that included commercial crime coverage.

A March 1998 audit uncovered unauthorized charges of $40,000. The president agreed to repay the charges within two weeks, but he did not do so. A March 1999 audit revealed that the president's personal charges on the credit card had increased to more than $225,000. In June 1999, the insured notified the insurer of loss and submitted a proof of claim to the insurer, which denied coverage and filed a declaratory judgment action. This was denied, but following a bench trial, the trial court entered judgment for the insurer because of late notice.

The Supreme Judicial Court of Maine affirmed. The policy provided that the insurance was cancelled as to any employee "immediately upon discovery" by the insured of any dishonest act committed by that employee. It also required the insured to give notice of loss as soon as possible and to submit a proof of loss within 120 days. The court concluded that the evidence supported the trial court's determination that the insured had discovered the dishonest conduct in March 1998, when the president had agreed to repay the unauthorized charges within two weeks. The court held that coverage for the president terminated at that time.

Proof of loss filed in June 1999 was untimely, the court concluded, and that the insurer was prejudiced by the delay.

Acquisition of insured's stock by another bank was "taking over" of insured and terminated coverage.

In *American Casualty Co. of Reading, Pennsylvania v. Etowah Bank*,[19] American Casualty, a CNA Cos. entity, insured Etowah Bank under a financial institution bond. It denied coverage for an employee dishonesty loss discovered during the term of the bond because Etowah had been "taken over" by Regions Financial Corp. 30 days before the loss was discovered. Regions had purchased 100 percent of Etowah's stock. American Casualty filed a complaint for declaratory judgment.

On cross motions for summary judgment, the district court found that the termination provision of the bond was ambiguous and entered judgment for the insured. The 11th Circuit reversed and instructed the lower court to enter judgment for the surety.

Under its terms, the bond terminated "as an entirety" on the "taking over" of the insured by another institution. The appeals court held that Etowah had been taken over when Regions purchased 100 percent of Etowah's stock and Etowah became its wholly owned subsidiary. It concluded that the term "taking over," as used in the bond, is not ambiguous and occurs when a financial institution acquires more than 50 percent of the stock of another institution.

Etowah argued that a "taking over" by Regions never occurred because Regions

18. 793 A.2d 495 (Me. 2002).
19. 288 F.3d 1282 (11th Cir. 2002).

did not assume control of Etowah's "core functions," that Etowah continued to operate as before under the same by-laws, and that it maintained separate books and records, with management remaining substantially unchanged. Turning back this argument, the court observed that the "core functions" test is used to determine whether a receiver or regulator has assumed control over, and has thus taken over, a failed financial institution, where stock ownership has not changed. That test, the court stated, does not apply in cases involving the purchase of stock by another institution.

E. Third-party Rights

Employee dishonesty coverage did not inure to insured's creditor.

In *O/E Systems Inc. v. Inacom Corp.*,[20] the plaintiff leased computer equipment to Inacom. After Inacom filed a petition in bankruptcy, the leased computer equipment could not be located. The lessor assumed that the equipment was misappropriated by Inacom's former employees and asserted a claim under Inacom's commercial crime policy, The federal district court in Delaware granted the insurer's motion to dismiss.

Under the terms of the policy, coverage was provided only for the insured's benefit and did not inure to any other person or organization. The court held that the plaintiff therefore could not make a claim directly under Inacom's policy because it was not a named insured under the policy or a third-party beneficiary, nor was it an assignee or judgment creditor of the insured.

F. Recoveries

Made-whole doctrine superceded ambiguous subrogation clause in policy.

In *Kanawha Valley Radiologists Inc. v. One Valley Bank N.A.*,[21] CNA Cos. intervened in a lawsuit to obtain a share of the proceeds of a settlement Kanawha Valley (KVA), its insured, had negotiated with One Valley Bank to obtain partial restitution for funds embezzled from KVA by one its employees. The trial court determined that the common law made-whole doctrine prevented CNA from enforcing its subrogation rights until the insured was fully reimbursed for its loss. The appellate court affirmed,

CNA insured KVA under a business package policy that included coverage for "employee dishonesty." KVA's employee embezzled $2.3 million over a 10-year span, about $268,000 of which occurred during the term of the policy. CNA paid the $50,000 policy limit, and KVA initiated lawsuits against those responsible for the loss, including One Valley Bank.

CNA maintained that the subrogation provision of the policy entitled it to a share of the recoveries. The provision stated that "amounts paid in excess of the payments under the policy shall be reimbursed up to the amount paid by those, including you, who made such payments." Finding the provision to be ambiguous, the West Virginia Supreme Court of Appeals instead applied the common law made-whole doctrine, under which an insured must be fully reimbursed before subrogation rights arise. The court noted that the doctrine may be overridden by valid contract, but held that the contractual provision was ambiguous and therefore invalid,

IV. SURETIES' REMEDIES

Power plant operator that paid defaulting contractor subs and suppliers is not volunteer and is allowed recovery under performance bond.

Ordinarily, sureties are clamorous proponents of the doctrine of equitable subrogation, but in *Federal Insurance Co. v. Maine Yankee Atomic Power Co.*,[22] equitable subrogation was used against a surety.

In 1998, Maine Yankee decided to decommission one of its nuclear plants. It hired Stone and Webster Engineering to do the job at a cost of $250 million. Under the

20. 179 F.Supp.2d 363 (D. Del. 2002).
21. 557 S.E.2d 277 (W.Va. 2001).
22. 183 F.Supp.2d 76 (D. Me. 2001).

contract, performance bonds in the amount of 15 percent of the contract price were secured from Federal Insurance Co.

By 2000, the power company was having serious concerns with the contractor's solvency, and in May of that year a default was declared. By that time, approximately $12 million worth of labor and material from the contractor's subs and suppliers had accrued but not yet been paid. However, not all these amounts were overdue, and no claim was made that the surety defaulted on its payment bond obligations.

The power company was apparently quite anxious to complete the project. To guard against delay, it negotiated something called an interim service agreement that allowed Stone & Webster to continue work on a reimbursable cost basis, with payments going from Maine Yankee to subs and suppliers directly. Federal concurred and, in fact, even signed the agreement, which, however, contained a general reservation of rights clause.

Maine Yankee then paid the subs and suppliers approximately $12 million for accruals that predated the default. Later, it decided to complete the decommissioning project itself and made a formal claim against Federal for the full amount of the performance bond. There was at least agreement that the obligee had no right to recover under the payment bond. Subcontractors and suppliers were paid as part of the agreement, and claims under the payment bond were never presented.

Although the federal district court in Maine referred to the route of recovery as "equitable subrogation," its analysis soon turned to an "unjust enrichment" claim. It stated:

> Since the [payment] bond amounts never actually came due, at bottom Maine Yankee is arguing that Federal Insurance has been unjust enriched—that by virtue of Maine Yankee's payments to subcontractors and suppliers Federal Insurance has saved the $12,000,000 it would ultimately have had to pay them under the payment bond a risk for which Federal Insurance received the premium.[23]

The theory is then referred to as one of "equitable subrogation combined with unjust enrichment."

The court had no trouble in finding that Maine Yankee unjustly enriched Federal Insurance, basically reasoning that it had paid sums that otherwise would have been payable under the payment bond, despite the fact that no claims were ever presented. It also refused to preclude recovery under the doctrine of volunteerism, find this to be something requiring strict interpretation as well as good and sound economic reasons for Maine Yankee doing what it did. In addition, although dealing with a given subject matter under an express contract would have precluded recovery under Maine common law, the court found this not to be the case.

Award of attorneys' fees upheld pursuant to indemnity agreement where challenge was non-specific.

Schaefer v. Spider Staging Corp.[24] did not involve a surety. In fact, it was a personal injury case, but it did involve a construction project and a contractual indemnity agreement.

Two roofers employed by Schaefer and Sons Roofing Inc. were hurt on the project when a scaffolding platform rented from Spider collapsed. In the paperwork on the project the roofer agreed to indemnify the scaffolding company even for its own negligence. The relevant clause was one to indemnify and hold harmless from any and all claims, actions, suits, proceedings, costs, expenses, damages and liabilities, including costs of suit and attorneys' fees.

The trial court had made fairly substantial awards. In one action, $315,358 was recovered; in another, the fee bill was $55,752. Schaefer Roofing appealed on the grounds of reasonableness.

On appeal, the Eighth Circuit initially considered the standard of review and refused to scrutinize the listing of services

---

23. *Id*. at 76.

24. 275 F.3d 735 (8th Cir. 2002), *panel and en banc rehearing denied*, 2002 U.S.App. Lexis 2341.

rendered, instead deferring to the "careful consideration" of the court below. In addition, Schaefer made "no specific challenge to [the] records except an unsupported assertion that the hourly billing rates were excessive." It was held that lacking a detailed challenge, the district court did not abuse its discretion in accepting the submission of fee bills.

Disputes over the recovery of fees and costs are common in indemnity battles, and the case provides further corroboration for the premise that in indemnity battles an indemnity agreement means what it says.

Surety liable for interest and costs in excess of sum of penal bond; surety's liability for interest arises at date of conversion of property, not from date of notice or demand on surety.

In *In the Matter of the Conservatorship of Huerta*,[25] the Kansas Supreme Court ruled that a lower court was within its authority to impose a judgment of interest against three sureties in excess of the penal sum of their conservatorship bonds. The court went a step further and held that the sureties were liable for interest dating back to the date of the conversion of the wards' assets, not just from the date that the sureties received notice of the loss or demand under the conservator's bond.

Six cases were consolidated, all of which revolved around claims by successor conservators against former conservators who were unable to account for all of the assets of their respective wards. Successor conservators filed suit against both the principals and sureties—St. Paul, USF&G, and Old Republic—as a result of the principals' theft of funds belonging to the wards. Judgments were rendered in each case against the principals and the sureties in the amount of each wards' loss, plus interest from the dates of the conversions. All the judgments, except one, exceeded the amount of the penal sums of the bonds when interest and the fees of the successor conservators were included in the judgment amount.

The sureties raised two defenses. First, they argued that Kansas state law limits their liability to the amount of the bond. In response to this argument, the successor conservators pointed to well-settled Kansas law which, they claimed, followed the majority view that while the amount of the penal sum of a bond may not be enlarged, a surety may be required to pay prejudgment interest and costs of suit even if they exceed the amount of the bond. After an exhaustive analysis of the cases cited by the successor conservators, the court agreed with their position and acknowledged that Kansas state law has allowed the award of prejudgment interest against a surety since 1885.

Next, the sureties argued that while an award of interest from the date of the defalcation may be authorized by Kansas state law, case law does not mandate such an outcome. The sureties claimed that the relevant case law allows for an award of interest from the time that the sureties' duty to discharge the liability "matured." In other words, they claimed that interest cannot be charged against them until the accounts of the wards are settled and the assets delivered to the wards, or until such time as the conservators are discharged from their duties.

The successor conservators argued that it was beyond question that a principal who converts funds is liable from the date of the conversion. The court agreed, noting that Kansas law acknowledged that a surety's liability is dependent on the liability of its principal. The court also stated that the case law relied up was consistent with the current state of law allowing a surety to step into the shoes of the conservator in order to fulfill the conservator's duties should the conservator fail to do so. The court also recognized that in conversion actions, the general rule is that interest is recoverable from the date of the conversion.

There is special relationship between principal debtor and surety.

In *Good v. Holstein*,[26] the Superior Court of Pennsylvania held that a surety who

25. 41 P.2d 814 (Kan. 2002).
26. 787 A.2d 426 (Pa.Super. 2001).

held a first mortgage was satisfied when a property was attributed its fair market value sufficient to cover the entire amount of a surety agreement. Reversing the trial court, the court concluded that the law has recognized a special relationship between the principal debtor and his surety based on reciprocal duties and mutual confidence. The core of this special relationship is the surety's obligation to repay the debt of the principal debtor if the latter defaults due to inability to repay the creditor. Conversely, a creditor has a duty to a surety to discharge liens on the mortgaged property in order of seniority.

In this case, the holder of a first mortgage, who was also the owner of a corporation that held the second mortgage, filed a confession of judgment action against the sureties of the first mortgage, after the second mortgage was foreclosed and the property was sold at sheriff's sale. The sureties filed an action in assumpsit, seeking payment on the surety agreement. The trial court entered judgment on finding that the sureties were personally liable to the owner corporation for the amount in default.

On the appeal, the Superior Court held that the corporation was the alter ego of sole owner for purposes of the sale of the property on which the corporation held the second mortgage, and also that a surety who held a first mortgage was satisfied when property was attributed its fair market value.

DECISIONS

Current Decisions

By Carol McHugh Sanders

CARMAKERS' DAMAGES

$290 Million Punitive Award Against Ford Stands

Voting 4-3 and, according to a story in *The Recorder* [San Francisco], causing corporations nationwide to issue a "collective gasp," the California Supreme Court declined to review or depublish a California Court of Appeal decision that imposed a $290 million punitive award against Ford Motor Co. in a products liability case in which three family members died in a rollover crash. 2002 Cal. Lexis 7254. The court's order lets stand the intermediate appellate court's decision and lengthy opinion in *Romo v. Ford Motor Co.*, 122 Cal.Rptr.2d 139 (Cal.App. 2002), which reversed the trial court's order allowing a new trial on punitive damages based on juror misconduct.

The case arose from an accident a decade ago involving a 1978 Ford Bronco. Both Romo parents and one child were killed when the vehicle rolled over several times. The suit alleged that the Bronco was defectively designed because only the front one third of the roof had steel support, while the remainder was made of fiberglass, which easily collapsed in the rollover accident.

After a four-month trial in 1999, a jury awarded the three surviving Romo children $6.226 million in compensatory and $290 million in punitive damages. Granting Ford's post-trial motion for a new trial on punitive damages based on juror misconduct, the trial court also reduced the compensatory award to $4.935 million.

Juror declarations filed at the post-trial stage revealed that one juror, during deliberations on the malice aspects of the case, commented that she had watched a television news program reporting on fires that occurred in older Ford Mustangs. She recounted to the jury that the former Ford chairman had said that the company would rather contest or settle the fire-related lawsuits than recall and fix all the vehicles. The jury foreperson, who was a deputy district attorney, told the juror that the news program was not evidence in their case and should not be discussed further, according to the juror declarations.

Another juror, Ford alleged, engaged in misconduct by recounting during deliberations a dream she from the night before in which a Ford Bronco rolled over, killing her own children and many others while Ford representatives stood by questioning the proof of the event. Her discussion of the dream occurred after the jury decided compensatory damages and before the vote on malice. Several other jurors stated that this juror repeatedly said during deliberations that the jury must "save the babies" by finding Ford liable. The jury voted 9-3 on the issue of malice and the amount of punitive damages.

The Court of Appeal, in an opinion by Judge Vartabedian, found no juror misconduct had occurred and reversed the trial court's order. Nothing in the trial record indicated that the court should reject the normal presumption that the jury followed

the court's instructions, he stated, adding that the trial court, several days into the jury deliberations and after widespread news coverage about a large verdict against General Motors, admonished the jury to consider only the evidence presented at the trial and to ignore any news accounts concerning their case or any other case. The presumption of prejudice from the one-time mention of the television news program was rebutted by the record, the court stated.

The court also treated the juror's discussion of her dream as within the realm of a "permissible rhetorical device" used to express her fears of similar accidents. The collective process that makes up a jury deliberations, the court explained, disabused the two jurors of any "misconceptions" they may have had about their duty as jurors to follow the law and consider only evidence presented at the trial, which rebuts any presumption of prejudice.

Ford also argued, but to no avail, that the plaintiffs had not proved that it acted with malice in designing and manufacturing the Bronco. The design and production of the Bronco itself was the despicable conduct, the court said. "[W]e think it obvious that putting on the market a motor vehicle with a known propensity to roll over and, while giving the vehicle the appearance of sturdiness, consciously deciding not to provide adequate crush protection to properly belted passengers . . . constitutes despicable conduct," the court determined.

The court pointed out other evidence that tipped the scales against Ford on the "despicable scale," including that the company knew truck-based sport utility vehicles roll over at a higher rate than passenger cars; the company's safety engineers had concluded that no utility vehicle should be produced without a roll bar; and Ford's own testing, after the first generation of Broncos was on the road, showed that the roof failed to meet the company's safety standards, and it began including steel reinforcement in all Broncos built after 1980.

As for the $290 million punitive award, Ford argued that it was so excessive that it violated due process rights. Although no other California case approached the size of this punitive award, the Court of Appeal held it was not excessive. Using the guideposts set by the U.S. Supreme Court in *BMW of North America Inc. v. Gore*, 517 U.S. 560 (1996), the court condemned Ford's conduct as very reprehensible in putting thousands of lives at risk. In the court's view, there was not a wide disparity between the actual harm suffered by the Romo family and the damages rendered, and Ford should have been on notice that punitive damages that amounted to 1.2 percent of the company's net worth were a possibility in this trial.

Chrysler Fails to Reverse $3 Million Punitive Award

In another case involving a much smaller punitive damages award, Chrysler lost out before the Sixth Circuit in its bid to overturn a jury verdict. *Clark v. Chrysler Corp.*, 310 F.3d 461 (6th Cir. 2002).

The jury award in this case also arose from a fatal crash in which Charles Clark was driving his Dodge Ram truck when he was hit in October 1993 by a state police car. It collided with the left front fender of Clark's truck, causing the vehicles to rotate and "side slap" after impact. Clark, who was not wearing a seat belt, was ejected from the truck, thrown onto the grass median and died six hours later from the injuries. Neither the police officer nor Clark's two passengers were seriously injured.

Clark's wife alleged in her products liability suit that Chrysler's lock latch on the Ram's doors was defectively designed, as it did not hold the door shut during the accident. The jury found Chrysler and Clark were each 50 percent at fault, so that the jury's $471,258 compensatory award was cut in half in the judgment for Clark, while its $3 million in punitive damages stood.

Affirming, the Sixth Circuit determined in an opinion by Judge Oliver that both of Clark's expert witnesses demonstrated that their scientific testimony was sufficiently reliable under standards set in *Daubert v. Merrell Dow Pharmaceuticals Inc.*, 509

U.S. 579 (1993). Clark's lock latch expert testified that the 1992 Dodge Ram did not have a state-of-the-art or state-of-the-industry lock latch. He referred to several other lock latch examples in the industry that were state-of-the-art at the time that Clark's pickup truck was manufactured. His opinion that the lock latch was defective and unreasonably dangerous, the court determined, was based on a sufficiently reliable foundation, including his technical knowledge of automobile door latch systems, his extensive testing of door latch bypass failure, his familiarity with the Chrysler K latch and his examination of the latch in Clark's truck, as well as other K latches identical to the one involved in Clark's case.

Likewise, Clark's accident reconstruction expert also demonstrated sufficient reliability under the *Daubert* standards. That expert testified that the structure to which the truck's door attached when it closed, called a B-pillar, is the skeleton of the vehicle and typically would be reinforced. He said that the Dodge Ram lock latch was 40 years out of date and that the B-pillar was defectively designed because it was a single piece of sheet metal that had not been shaped and welded into a square box to provide structure, as was typical in the industry. This testimony had sufficient reliability, the court concluded, because the expert had an extensive background in automobile safety testing and had examined Clark's truck, the accident scene, the police report and the photographs. He also knew the state-of-the-art and state-of-the-industry standards in B-pillars at the time Clark's truck was built.

Chrysler also failed to persuade the Sixth Circuit that a new trial was needed based on testimony about four other substantially similar accidents and because the lower court refused to use a jury instruction on the presumption accorded to compliance with federal motor vehicle standards. Chrysler also struck out on its claim that the punitive award must be considered so excessive that it offends due process safeguards.

Concurring and dissenting, Judge Nelson said he was on board with the majority's opinion on the defective design issues but could not go along with the majority on the punitive damages issue. In his book, the issue of punitive damages should not have been submitted to the jury because Clark did not produce clear and convincing evidence that Chrysler was guilty of wanton or reckless disregard for the lives and safety of its customers.

To Judge Nelson's thinking, the record supported only a finding of "garden-variety negligence" on Chrysler's part. If Clark had used the seat belt that Chrysler provided, his life would have been spared, he wrote. "The hard truth, uncomfortable though it may be to say so, is that if anyone was reckless in this situation, it was Mr. Clark himself, not Chrysler," he concluded.

CLASS ACTIONS

District Court Off Track in Selecting Lead Plaintiff

A federal district court may get to pick the lead plaintiff in a securities class action, but not that plaintiff's counsel, according to a first impression decision from the Ninth Circuit that reversed the lower court's choice of lead plaintiff. The petition for a writ of mandamus drew an amicus curiae brief from the Securities and Exchange Commission, supporting the party appointed lead plaintiff, and an amicus brief from two large institutional investors—the California Public Employees Retirement System and Barclays Global Investors—supporting the district court's position.

The class action before the Ninth Circuit, *In re Cavanaugh*, 306 F.3d 726 (9th Cir. 2002), was one of more than 20 securities fraud complaints filed in the U.S. District Court for the Northern District of California based on a dramatic drop in late 2000 in the share price of a company in the telecommunications business, Copper Mountain Networks Inc., whose stock price plunged in the fourth quarter of 2000 from $125 to $10 per share after it an-

nounced that its revenues and earnings for that quarter had declined, contrary to earlier projections.

The district court announced plans to consolidate the numerous class actions and to appoint a lead plaintiff, as allowed under the Private Securities Litigation Reform Act of 1995 (PSLRA). Scheduling a case management conference, the court interviewed three parties who expressed an interest in becoming lead plaintiff: William A. Chenoweth, an accountant who lost an estimated $295,000 on the stock's decline; Quinn Barton, a self-employed investor who lost about $59,000; and five businessmen, led by David Cavanaugh, who each lost between $462,000 and $943,000 for a collective loss of $3.327 million.

At the case management conference, the district court queried all three candidates about how they chose their attorneys and negotiate their fee agreements. The Cavanaugh group already had retained Milberg, Weiss, Bershad, Hynes & Lerach, arguably the best-known plaintiffs' securities litigation firm in the nation, under a fee agreement that would pay it a percentage of the total recovery, a sum that would increase with the size of the recovery, topping out at just over 30 percent.

The second lead plaintiff candidate, Barton, had retained Beatie & Osborn, a small New York law firm, under a fee agreement that would pay between 10 to 15 percent of the recovery, with an $8 million cap. The third candidate, Chenoweth, had not retained counsel.

The court found the Cavanaugh group presumptively the most adequate plaintiff under the PSLRA standard because it had the largest financial stake in the controversy, but it concluded that Barton had rebutted that presumption by showing he had a more advantageous attorneys' fee agreement. Referring to Milberg, Weiss, the court commented that the "well-recognized brand name in securities litigation" could not rationally explain the significantly larger fee compared to Barton's counsel. Disqualifying Chenoweth from consideration because he had not selected counsel, the court appointed Barton as lead plaintiff for the class.

On the Cavanaugh group's petition to the Ninth Circuit for a writ of mandamus, the appeals court reversed and remanded. In an opinion by Judge Kozinski, it held that the district court went way beyond the dictates of the PSLRA in selecting the lead plaintiff. That court, Judge Kozinski wrote, "quickly went off the statutory track" by engaging in a "free-wheeling comparison" of the parties competing for lead plaintiff. The only relevant comparison under the PSLRA's statutory scheme evaluates plaintiffs' financial interest in the outcome of the litigation, he stated.

The most capable plaintiff under the PSLRA is presumptively the one with the greatest financial stake in the outcome of the case, so long as he meets the typicality and adequacy requirements for a class representative under Rule 23 of the Federal Rules of Civil Procedure, the Ninth Circuit panel observed, and then other plaintiffs may then try to rebut the presumptive lead plaintiff's showing of typicality and adequacy under Rule 23. The Ninth Circuit rejected the lower court's view that a plaintiff's adequacy under Rule 23 can be measured in part by how good a fee deal he strikes with his attorneys. If the Rule 23 adequacy determination turns on which plaintiff has the cheapest deal, the court said that would pressure plaintiffs to pick a lawyer who offers the lowest fees, rather than counsel who they believe will do the best job for the class. Besides, the court added, the district court gets a say later in the ball game on attorneys' fees when it approves any class action settlement, which the appeals court noted is "virtually the universal case."

The presumptive lead plaintiff's choice of counsel and fee arrangement may be relevant, the court added, in ensuring that the plaintiff is not receiving preferential treatment in some back-door financial arrangement or has engaged a lawyer with a conflict of interest. "But this is not a beauty contest; the district court has no authority to select for the class what it considers to be the best possible lawyer or the lawyer offering the best possible fee schedule,"

the court stated. "Indeed, the district court does not select class counsel at all."

The Ninth Circuit also rejected amicus SEC's contention that the PSLRA raised the adequacy bar for lead plaintiffs to ensure that the most sophisticated investor available garners that lead role. The statute may have heightened the pleading requirements and otherwise strengthened the chances of an institutional investor serving as lead plaintiff, the court stated, but it did not up the ante on the Rule 23 adequacy requirements. It does not give district courts the sweeping authority to deny a plaintiff the role of class representative because the court disagrees with his choice of counsel, the court held.

Granting the writ of mandamus, the Ninth Circuit instructed the lower court to vacate its order appointing Barton as lead plaintiff and to appoint the Cavanaugh group to that role if no other party rebuts the presumption that the group is the most capable of adequately representing the class.

Concurring in the judgment, Judge Wallace wrote separately to note that the majority's opinion neither determined its own jurisdiction for the extraordinary remedy sought nor confined itself to the questions posed. On the jurisdictional issue, he resolved that a "clear procedural error" had occurred in the lower court that would warrant a mandamus. He chided the majority, however, for interjecting "ruminations on the quality of the firms selected by the prospective lead plaintiffs in this case" and for otherwise putting forth "broad-ranging dicta" on what should occur at the lower court on remand.

CLASS ACTIONS

Lawyer Liable for Debt Collection Violations

A Virginia lawyer who sent dunning letters to Illinois residents to collect on delinquent accounts for a large credit card company is liable under the federal debt collection laws because he did little more than lend his name and firm letterhead to the company's collection effort, the Seventh Circuit held in *Nielsen v. Dickerson*, 307 F.3d 6223 (7th Cir. 2002).

The court affirmed the trial court's summary judgment in favor of a class of debtors who alleged that David D. Dickerson, a Virginia-licensed attorney, violated the Fair Debt Collection Practices Act (FDCPA). Each class member had been a GM credit card holder who had received a letter on Dickerson's law firm letterhead between September 22, 1997, and July 15, 1999, about his or her delinquent account. The district court determined that Dickerson's minimal involvement in preparing the letters rendered them misleading in violation of Section 1692e(3) of the FDCPA. 1999 U.S.Dist. Lexis 13931.

The letters, the district court ruled, falsely implied to the debtor that an attorney had become professionally involved in the collection, violating Section 1692e(10)'s ban on using any false representation or deceptive means in collecting a debt. After the district court granted summary judgment on liability, the parties reached a settlement that reserved the defendants' right to appeal the liability ruling.

Dickerson argued on appeal that he was meaningfully involved in sending out the delinquency letters. Household Bank, which had issued the GM cards, sent Dickerson a list of about 2,000 debtors each month, for which he was paid $2.45 per account. He pointed out on appeal that he briefly reviewed the data printouts from Household each month. His staff also checked the firm's database to see if the account holder's name showed up among recent bankruptcy court filings and to determine if the firm had already sent a letter to that person. The firm's staff also checked the debtors' addresses to be sure no one resided in one of three states that prohibited the type of letter Dickerson intended to send.

After the firm completed its three-part review, the data was turned over to a bulk mailing facility to send out on the firm's letterhead with a facsimile of Dickerson's signature. The letters advised the debtors to

contact Household about the delinquency and make payments directly to GM card. If a debtor contacted Dickerson's office by mail, that letter was forwarded to Household. Telephone calls from debtors were taken either by Dickerson himself, who advised the caller to write a letter, or messages were taken by his staff and then forwarded to Household for handling. Dickerson never instituted legal action against any GM debtors.

In an opinion by Judge Rovner, the Seventh Circuit held that Dickerson's letters falsely suggested that an attorney had become actively involved in GM's debt collection efforts. The work that Dickerson and his staff performed for GM in an "assembly-line fashion" was nothing more than ministerial, in the court's view; the dunning letters basically were form letters prepared and issued en masse. The undisputed facts showed the court that Dickerson brought no professional legal judgment to bear on the effort.

Household argued on appeal that it could not be liable as a "debt collector" under the FDCPA because it had not falsely used Dickerson's name in its debt-collecting efforts. The court disagreed. It deemed Household, although the creditor, to be a debt collector because it used Dickerson's name and letterhead to give the false impression to its debtors that an attorney was involved. Dickerson did not individually assess the status or validity of the debts, relying on Household's judgment on those matters. If a debtor who received the past-due letter contacted Dickerson's firm, rather than GM directly, as instructed in the letter, the law firm was not authorized to negotiate a payment plan, settle the debt or take legal action against the debtor.

The $2.45 per account flat-rate fee arrangement also indicated to Judge Rovner that little actual legal work was expected in preparing the past-due letters. "The fixed and quite modest nature of Dickerson's remuneration strongly suggests that Household was paying for the marquee value of Dickerson's name rather than his professional assistance in the collection of its debts," she wrote. Finding that Household was the true source of Dickerson's letters, the court held that Household shared Dickerson's liability as a debt collector under Section 1692a(6) for violating other sections.

The Seventh Circuit also saw little merit in Household's claim that it did not intentionally violate the FDCPA because it had made a bona fide error in legal judgment. Household's bona-fide error defense was doomed, the court said, because its actions plainly contravened the court's opinion in *Avila v. Rubin,* 84 F.3d 222 (7th Cir. 1996), in which the court recognized that a delinquency letter from an attorney conveys authority and implies that the attorney supervised or actually controlled the procedures behind the dunning letter. To avoid liability for misrepresentations with such a letter, the attorney must have some professional involvement with the debtor's file. Since *Avila* was nearly a year old when Household retained Dickerson, the credit company could not avail itself of the bona fide error defense.

EMPLOYMENT LAW

Sidley, Austin Firm Must Turn Over More Information

A Chicago-based law firm must comply more fully with a subpoena in an Equal Employment Opportunity Commission (EEOC) investigation to determine whether 32 demoted partners in fact were employees under the Age Discrimination in Employment Act (ADEA). The Seventh Circuit did not resolve whether the former partners at Sidley & Austin were employees, but only that there is enough doubt about whether they are covered by the age discrimination laws to entitle the EEOC to greater compliance with its subpoena. *Equal Employment Opportunity Commission v. Sidley, Austin, Brown & Wood,* 2002 U.S.App. Lexis 22152).

A concurring judge noted that the U.S. Supreme Court has granted certiorari in a case from the Ninth Circuit that may resolve some or all of the problems that govern the classification of Sidley's members.

Wells v. Clackamas Gastroenterology Associates P.C., 271 F.3d 903 (9th Cir. 2001), *cert. granted*, No. 01-1435, October 1, 2002 (summary at 71 U.S. Law Week 3062). The Ninth Circuit held in *Clackamas* that any person classified as an employee for purposes of state law necessarily is an employee for purposes of federal law.

The EEOC pursued information from the law firm now known as Sidley, Austin, Brown & Wood after the firm demoted the 32 equity partners in 1999 to "counsel" or "senior counsel" status. The commission subpoenaed documents relating to whether those partners were covered by ADEA, which protects employees, but not employers, from age discrimination. The commission also sought information about whether Sidley may be forcing other partners to retire at a set age, contrary to federal anti-discrimination laws that abolished mandatory retirement.

On the commission's motion to enforce its subpoena, the federal district court ordered the firm to comply fully. 2002 U.S.Dist. Lexis 2113.

On appeal, Sidley maintained that it produced enough information to show that the 32 lawyers were bona fide partners before their demotion and, as such, were employers not covered by ADEA. The firm also asserted that the question of whether the 32 demoted partners are within the ADEA's coverage is jurisdictional, which once answered against the commission, requires it to stop investigating.

The Seventh Circuit, in an opinion by Judge Posner, said the firm could "obtain no mileage" by characterizing the coverage issue as jurisdictional. EEOC could pursue information as to whether the 32 demoted partners were employees under the ADEA because it is entitled to investigate sufficiently to determine whether it should proceed to the enforcement stage, the court stated.

While Sidley may have shown that the 32 lawyers were partners, it did not necessarily mean that they were employers exempt from ADEA coverage, Judge Posner wrote. He noted that the firm is governed by a 36-member executive committee that appoints its own members, rather than standing for election before all 500 partners in the firm. That committee makes all major decisions for the firm and delegates to non-committee members some powers to hire, fire, promote and determine compensation of subordinates. The executive committee also sets partners' income, based on each partner's percentage of the firm's over-all profits.

Perhaps the "most partneresque feature" of the 32 demoted lawyers relationship with the firm was their personal liability for the firm's debts, Judge Posner noted. Yet, that exposure to liability should not be decisive as to whether they are employers, he continued, because they had no power over their own fate at the firm. The two groups—partners under state law and employers under the ADEA—may not coincide, the court stated.

Vacating the district court's order, the Seventh Circuit said that once the firm fully complies with the subpoena concerning ADEA coverage, the lower court should then decide whether the 32 partners are arguably covered by the ADEA.

Concurring in the judgment, Judge Easterbrook said he would count the 32 lawyers as "real partners" and consequently not employees under the ADEA. He found the suggestion that one can be a partner under normal agency principles and still be an employee because of a "federal law override" incompatible with the U.S. Supreme Court's discussion of employees under the Employee Retirement Income Security Act in *Nationwide Mutual Insurance Co. v. Darden*, 503 U.S. 318 (1992). *Darden*, he noted, held that the circularity of ADEA's definition of employee should be fixed by incorporating into federal law the traditional state agency law criteria for identifying master-servant relations.

Illinois treats participation in profits as the defining characteristic of a bona fide partner, Judge Easterbrook noted, and that would make the 32 demoted partners employers. "Anyway, it makes both linguistic and economic sense to say that someone who is liable without limit for the debts of an organization is an entrepreneur (a prin-

cipal) rather than an 'employee' (an agent)," he wrote.

INSURANCE COVERAGE

Insurer Must Defend Hospital Against Defamation Claim

An insurer has to defend a New York-based hospital and its staff in a defamation action brought by a doctor who had risen to the "limited public figure" status with his very vigorous campaign supporting midwifery at the facility. The New York Court of Appeals held in *Town of Massena v. Healthcare Underwriters Mutual Insurance Co.*, 2002 N.Y. Lexis 2729, that Healthcare must defend Massena Memorial Hospital in an underlying federal lawsuit the doctor filed alleging a host of wrongs, including defamation.

In the underlying action, Dr. Olof Franzon, who operated a women's medical and surgical health care office, filed a federal court complaint against the hospital, its board of managers and various physicians and hospital executives. He alleged that the defendants conspired to deprive him of his civil rights under the First and 14th Amendments by trying to "excommunicate him from, and ruin him, in the Massena medical community." He also charged that the hospital and medical personnel disparaged him in internal reviews and to his patients, refused to renew his hospital privileges and defamed him.

In the action that reached the New York Court of Appeals, the Town of Massena, which owned the hospital, sought a declaration that three insurers owed it a defense in the federal action. The trial court found that all three insurers owed a duty to defend. The Appellate Division reversed, holding that coverage for the alleged wrongs were either specifically excluded under the applicable policies' provisions or were intentional and therefore excluded as a matter of public policy. 724 N.Y.S.2d 107 (App.Div. 3d Dep't 2001). The appeal to the state's high court drew amicus curiae briefs from the Medical Society of the State of New York and the Healthcare Association of New York State.

The Court of Appeals concluded that one insurer is obligated to defend the hospital and its employees while the other two insurers are off the hook, based on specific policy exclusions. The court, in an opinion by Judge Smith, held that Healthcare Underwriters must defend under the personal injury liability policy it had in place with the hospital. That policy obligated Healthcare Underwriters to provide the hospital a defense for all personal injury damages arising from various acts, including libel, slander or other defamatory or disparaging material. The insurer argued that it did not have to defend because the policy excluded coverage for allegations of defamatory statements made within a business enterprise with knowledge of their falsity.

The federal district court in Franzon's underlying action held that he was a limited public figure who must prove recklessness as to the truth of the statements made, but not knowledge of their falsity. The state Court of Appeals held that even if the allegedly defamatory statements concerned Franzon's medical practice as a business enterprise and were intentionally and maliciously made, there was no allegation that the statements were made with knowledge of their falsity. It added that since Franzon is a limited public figure, actual malice requires only recklessness as to the truth of the statements and not knowledge of their falsity. Thus, defense coverage is proper based on the policy terms, the state high court held.

The insurer also argued that it had no duty to indemnify because the allegations of malice were equivalent to allegations of intentional wrongdoing. Because of Franzon's status as a limited public figure, he could recover on his defamation claim if he established that the hospital and its staff's allegedly defamatory statements were made with reckless disregard of their truth, the court stated, adding that such defamatory statements would be covered by Healthcare Underwriters' policy and would not be precluded by public policy.

JURY INSTRUCTIONS

Instruction Based on Store's Safety Manual Improper

The Indiana Supreme Court reversed a $600,000 jury award because of an improper jury instruction incorporating a Wal-Mart employee manual that set a standard of care higher than the ordinary care required in the negligence suit at issue. Reversing the jury verdict, the court determined in *Wal-Mart Stores, Inc. v. Wright*, 774 N.E.2d 891 (Ind. 2002), that the instruction set a subjective, rather than objective, standard of care in the slip-and-fall case.

Ruth Ann Wright sued Wal-Mart, alleging she was injured when she fell on water in the lawn and garden corral outside the Wal-Mart store in Carmel, Indiana. Portions of the store's employee manual, detailing procedures on handling spills and other floor hazards, were admitted into evidence at the jury trial. Wal-Mart hotly contested the applicability of the manual to the open-air lawn and garden corral. A Wal-Mart employee, who was just arriving for work and witnessed Wright fall, testified that she routinely swept or squeegeed water from the corral floor as needed.

One jury instruction told jurors they could consider the violation of any of the store's own rules, along with all the other evidence, in determining whether Wal-Mart was negligent. The instruction also provided that the violation of these rules was a "proper item of evidence tending to show the degree of care recognized by Wal-Mart as ordinary care under the conditions specified in its rules, policies, practices and procedures."

The jury returned a $600,000 verdict in favor of Wright, which was reduced to $420,000 based on her 30 percent comparative fault. The Indiana Court of Appeals affirmed. 754 N.E.2d 1013 (Ind.App. 2001).

The state supreme court, in an opinion by Justice Boehm, reversed, agreeing with Wal-Mart's argument that the jury instruction based on its store manual set a higher standard of care than ordinary care in the negligence action. Wal-Mart, the court held, correctly argued that its rules and policies may exceed what is required by ordinary care in a given situation, but that fact should not be used as evidence to create a separate or higher duty of care. "We think this rule is salutary because it encourages following the best practices without necessarily establishing them as a legal norm," the court stated.

The second problem with the instruction, the court held, was that it invited jurors to apply Wal-Mart's subjective view of ordinary care, rather than the objective standard set by external community demands. The store's belief that it should perform at a higher standard than objective reasonable care is not relevant to the jury's determination, the court stated, concluding also that the improper jury instruction could not be deemed harmless error.

SOVEREIGN IMMUNITIES ACT

Domain Name Game Goes International

An American-based Internet domain name registration company was not able to overcome sovereign immunity in its suit against the Republic of South Africa in a dispute over the use of a uniform resource locator on the Internet. In *Virtual Countries Inc. v. Republic of South Africa*, 300 F.3d 230 (2d Cir. 2002), the Second Circuit affirmed the U.S. District Court for the Southern District of New York's dismissal of the company's claims based on a lack of subject matter jurisdiction under the Foreign Sovereign Immunities Act of 1976 (FSIA).

Virtual Countries, a Seattle-based company that owns Internet domain names for various countries, had been using southafrica.com since October 1996 to publish travel news, weather and tourist information about the southern region of Africa. The Republic of South Africa owns southafrica.net.

Central to Virtual Countries' lawsuit was a press release that the Republic of South Africa issued in October 2000 an-

nouncing that it could be the first country in the world to claim the right to use its own domain name in the generic top-level domain of ".com." The release further stated that it intended soon to file an ownership claim to southafrica.com with the World Intellectual Property Organization, a United Nations agency that deals with intellectual property protection. The press release stated that sovereign countries have the first right to own their own domain names as national assets to help promote trade and tourism. South Africa also announced its intention to take up the issue before an international tribunal that supervises a non-binding arbitral system for resolving domain name disputes.

One week later, Virtual Countries filed suit in a U.S. federal court, asserting that the Republic of South Africa could not use southafrica.com and seeking to enjoin any arbitration or court proceeding in any forum worldwide that challenged its right to that name. Moving to dismiss the action, South Africa maintained that it was immune from suit in the United States because it was engaged in international diplomacy concerning the use of sovereign nations' domain names when it issued its press release.

Virtual Countries argued that the immunity veil did not protect South Africa because its acts outside the United States caused a direct effect in this country, a specific exception to immunity under Section 1605(a)(2) of the FSIA. The president of Virtual Countries filed a declaration stating that South Africa's press release had a "devastating" effect on his company's operations because it placed a cloud over its ownership of many domain names. As examples of the fallout it had suffered, the company noted that it had to sell switzerland.com and had lost a potential strategic alliance with a South African firm that feared reprisals from its country's government.

The federal district court in the Southern District of New York concluded that dismissal was appropriate because no exception in the FSIA destroyed South Africa's sovereign immunity. 148 F.Supp.2d 256 (S.D. N.Y. 2001).

Affirming, the Second Circuit held that South Africa's press release had no direct effect in the United States that would make the nation subject to jurisdiction in there under the FSIA. In an opinion by Judge Sack, the court concluded that any impact from South Africa's press release on Virtual Countries fell at the end of a long chain of causation, mediated by third parties' numerous actions. The news media's extensive coverage of South Africa's announcements and then investors' and potential partners' negative response to Virtual Countries intervened in any connecting chain between the press release and the company's financial difficulties. Virtual Countries' "expansive theory" that an American-based company's financial loss constitutes a direct effect in the United States was "plainly flawed," the appeals panel held.

TOBACCO TIMES

Nationwide Class Action Certified for Smokers

In a ruling that could have major ramifications for the tobacco industry, a U.S. district court judge in the Eastern District of New York on September 19, 2002, certified a nationwide class of plaintiffs to pursue strictly punitive damages against tobacco companies. *In re Simon II Litigation*, 212 F.Supp.2d 57 (E.D. N.Y. 2002), *confirmed and expanded as amended*, U.S.Dist. Lexis 19773, *reconsideration denied*, 2002 U.S.Dist. Lexis 22920.

Judge Jack Weinstein certified the class as a way to avoid a bunch of trials across the country resulting in unrelated punitive damage judgments in what he described as "massive and complex litigation." The class certified includes all smokers in the United States who have been diagnosed since April 9, 1993, with any of more than a dozen specified smoking-related illnesses. Diseases covered by the order include lung cancer, mouth cancer, chronic obstructive pulmonary disease and emphysema.

The class also includes smokers who resided in the United States at the time of their deaths and smoked cigarettes produced by any of the five major tobacco company defendants. The non-opt out class would exclude persons who already have obtained settlements or judgments against any defendant tobacco company. It also excludes anyone who is a member of the certified class in *Engle v. R.J. Reynolds Tobacco Co.*, No. 94-08273-CA-22, in the Circuit Court of the 11th Judicial Circuit, Dade County, Florida.

The order also excludes as class members anyone who should have reasonably realized that they had the a smoking-related disease prior to April 9, 1993, and anyone whose diagnosis of one of the specified diseases predates their use of tobacco.

REVIEWS

Reviewing the Law Reviews

Complied by Elizabeth M. Youngdale
Tarlton Law Library
University of Texas at Austin

This is a selective bibliography of current law review literature of interest to defense counsel. Main articles are identified by naming the author or authors. The designations "Note," "Comment," etc. are as listed in the publication, with the authorship, if given, shown in parentheses. Symposiums are generally shown by title.

U.S. and International

Damages

Jennifer K. Robbennolt, Determining Punitive Damages: Empirical Insights and Implications for Reform, 50 BUFF. L. REV. 103 (2002). Buffalo Law Review, State University of New York at Buffalo Law School, 605 John Lord O'Brian Hall, Buffalo, NY 14260.

Carrie L. Williamson, "But You Said We Could Do It!" Oil Companies' Liability for the Unintended Consequence of MTBE Water Contamination, 29 ECOLOGY L.Q. 315 (2002). Ecology Law Quarterly, 493 Simon Hall, University of California Boalt Hall, Berkeley, Berkeley, CA 94720.

Note (Adam W. Johnson), Injunctive Relief in the Internet Age: The Battle Between Free Speech and Trade Secrets, 54 FED. COMM. L.J. 517 (2002). Federal Communications Law Journal, Indiana University School of Law—Bloomington, 211 S. Indiana Ave., Bloomington, IN 47405.

Daniel A. Crane, Exit Payments in Settlement of Patent Infringement Lawsuits: Antitrust Rules and Economic Implications, 54 FLA. L. REV. 747 (2002). Florida Law Review, University of Florida Fredric G. Levin College of Law, 115 Holland Hall, Box 117637, Gainesville, FL 32611-7637.

Suan Perng Pan, Patent Damage Assessments after Rite-Hite and Grain Processing, 42 IDEA 481 (2002). IDEA, Franklin Pierce Law Center, Two White St., Concord, NH 03301.

Jennifer K. Robbennolt, Punitive Damage Decision Making: The Decisions of Citizens and Trial Court Judges, 26 LAW & HUM. BEHAV. 315 (2002). Law & Human Behavior, Box G-1126, Baruch College, 17 Lexington Ave., New York, NY 10010.

Lisa Litwiller, Re-examining Gasperini: Damages Assessments and Standards of Review, 28 OHIO N.U. L. REV. 381 (2002). Ohio Northern University Law Review, Claude W. Pettit College of Law, 525 South Main St., Ada, OH 45810.

Margaret Bull Kovera & Stacie A. Cass, Compelled Mental Health Examinations, Liability Decisions, and Damage Awards in Sexual Harassment Cases: Issues for Jury Research, 8 PSYCHOL. PUB. POL'Y & L. 96 (2002). Psychology, Public Policy & Law, American Psychological Association, 750 First St. N.E., Room 3082, Washington, DC 20002-4242.

Joel Stroud, Space Law Provides In-

sights on How the Existing Liability Framework Responds to Damages Caused by Artificial Outer Space Objects, 37 REAL PROP. PROB. & TR. J. 363 (2002). Real Property, Probate and Trust Journal, University of South Carolina School of Law, Main and Greene Streets, Room 301, Columbia, SC 29208.

Comment (John U. Bauco), Acquista v. New York Life Ins. Co.: Consequential Damages, Emotional Distress, and Protecting the Insured and the Insurer, 76 ST. JOHN'S L. REV. 201 (2002). St. John's Law Review, St. John's University School of Law, 8000 Utopia Pkwy, Jamaica, NY 11439.

Danielle Conway-Jones, Remedying Trademark Infringement: The Role of Bad Faith in Awarding an Accounting of Defendant's Profits, 42 SANTA CLARA L. REV. 863 (2002). Santa Clara Law Review, Santa Clara University, Santa Clara, CA 95053.

Douglas G. Smith, Application of Patent Law Damages Analysis to Trade Secret Misappropriation Claims: Apportionment, Alternatives, and Other Common Limitations on Damages, 25 SEATTLE U. L. REV. 821 (2002). Seattle University Law Review, 900 Broadway, Seattle, WA 98122.

M. Stuart Madden, Renegade Conduct and Punitive Damages in Tort, 53 S.C. L. REV. 1175 (2002). South Carolina Law Review, University of South Carolina School of Law, Columbia, SC 29208.

Noel Wise, Personal Liability Promotes Responsible Conduct: Extending the Responsible Corporate Officer Doctrine to Federal Civil Environmental Enforcement Cases, 21 STAN. ENVTL. L.J. 283 (2002). Stanford Environmental Law Journal, Stanford Law School, 559 Nathan Abbott Way, Stanford, CA 94305.

Comment (Theodore Eisenberg et al.), Reconciling Experimental Incoherence with Real-World Coherence in Punitive Damages, 54 STAN. L. REV. 1239 (2002). Stanford Law Review, Crown Quadrangle, Stanford, CA 94305-8610.

Mark A. Klugheit, "Where the Rubber Meets the Road": Theoretical Justifications vs. Practical Outcomes in Punitive Damages Litigation, 52 SYRACUSE L. REV. 803 (2002). Syracuse Law Review, Syracuse University College of Law, Syracuse, NY 13244-1030.

John R. Williams, Punitive Damages in Section 1983 Actions, 17 TOURO L. REV. 575 (2001).

Leon D. Lazer, The Latest Word from the Supreme Court on Punitive Damages, 18 TOURO L. REV. 107 (2001). Touro Law Review, Jacob D. Fuchsberg Law Center, Room 201, 300 Nassau Road, Huntington, NY 11743.

John Alan Cohan, Environmental Rights of Indigenous Peoples under the Alien Tort Claims Act, the Public Trust Doctrine and Corporate Ethics, and Environmental Dispute Resolution, 20 UCLA J. ENVTL. L. & POL'Y 133 (2002). UCLA Journal of Environmental Law & Policy, UCLA School of Law, Box 951476, 405 Hilgard Ave., Los Angeles, CA 90095-1476.

Lisa Litwiller, Has the Supreme Court Sounded the Death Knell for Jury Assessed Punitive Damages? A Critical Re-Examination of the American Jury, 36 U.S.F. L. REV. 411 (2002). University of San Francisco Law Review, 2130 Fulton Street, San Francisco, CA 94117.

Evidence

J. Alexander Tanford, The Ethics of Evidence, 25 AM. J. TRIAL ADVOC. 487 (2002).

Steven G. Drexler, A Guide for Submitting Questioned Documents and Handwriting Evidence, 26 AM. J. TRIAL ADVOC. 65 (2002). American Journal of Trial Advocacy, Cumberland School of Law of Samford University, 800 Lakeshore Drive, ROBH 307, Birmingham, AL 35229.

Mitchell L. Lathrop, The Changing Face of Expert Evidence, 52 FDCC Q. 409 (2002).

Frank H. Gassler, Dealing with Discovery in the Too Much Information Age, 52 FDCC Q. 513 (2002). FDCC Quarterly, Marquette University Law School, Box 1881, Milwaukee, WI 53201-1881.

Artemio Rivera, Testing the Admissibility of Trademark Surveys after Daubert, 84 J. PAT & TRADEMARK OFF. SOC'Y 661 (2002). Journal of the Patent and Trademark Office Society, Box 2600, Arlington, VA 22202.

Leonard Birdsong, The Exclusion of Hearsay Through Forfeiture by Wrongdoing—Old Wine in a New Bottle—Solving the Mystery of the Codification of the Concept into Federal Rule 804(b)(6), 80 NEB. L. REV. 891 (2001). Nebraska Law Review, University of Nebraska—Lincoln College of Law, Lincoln, NE 68583-0902.

Symposium, Translating Science into Law: Lessons from Doctors, Judges and Lawyers about the Use of Medical Evidence in the Courtroom, 36 NEW ENG. L. REV. (2002). New England Law Review, 154 Stuart St., Boston, MA 02116.

Joseph Sanders et al., Legal Perceptions of Science and Expert Knowledge, 8 PSYCHOL. PUB. POL'Y & L. 139 (2002).

Lloyd Dixon and Brian Gill, Changes in the Standards for Admitting Expert Evidence in Federal Civil Cases since the Daubert Decision, 8 PSYCHOL. PUB. POL'Y & L. 251 (2002).

Carol Krafka et al., Judge and Attorney Experiences, Practices and Concerns Regarding Expert Testimony in Federal Civil Trials, 8 PSYCHOL. PUB. POL'Y & L. 309 (2002). Psychology, Public Policy & Law, American Psychological Association, 750 First St. N.E., Room 3082, Washington, DC 20002-4242.

Jeremy C. Bucci, Revisiting Expert Testimony on the Reliability of Eyewitness Identification, 7 SUFFOLK J. TRIAL & APP. ADVOC. 1 (2002). Suffolk Journal of Trial and Appellate Advocacy, Suffolk University Law School, 120 Tremont St., Boston, MA 02108.

Insurance

Jennifer Kulynych & David Korn, Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule, 28 AM. J. L. & MED. 309 (2002). American Journal of Law and Medicine, American Society of Law, Medicine & Ethics, 765 Commonwealth Ave., Suite 1634, Boston, MA 02215.

Bradley C. Nahrstadt & Christina D. Ketcham, A Primer on Defending Breast Cancer Litigation, 25 AM. J. TRIAL ADVOC. 451 (2002). American Journal of Trial Advocacy, Cumberland School of Law of Samford University, 800 Lakeshore Drive, ROBH 307, Birmingham, AL 35229.

Yu-Ping Liao & Michelle J. White, No-Fault for Motor Vehicles: An Economic Analysis, 4 AM. L. & ECON. REV. 258 (2002). American Law and Economics Review, Box 208245, 127 Wall St., New Haven, CT 06520.

Robert W. Woody, Health Information Privacy: The Rules Get Tougher, 8 CONN. INS. L.J. 211 (2001). Connecticut Insurance Law Journal, University of Connecticut School of Law, 65 Elizabeth St., Hartford, CT 06105.

Benjamin J. Richardson, Mandating Environmental Liability Insurance, 12 DUKE ENVTL. L. & POL'Y F. 293 (2002). Duke Environmental Law & Policy Forum, Duke University School of Law, Durham, NC 27708.

Stephen J. Henning & Daniel A. Berman, Mold Contamination: Liability and Coverage Issues: Essential Information You Need to Know for Successfully Handling and Resolving Any Claim Involving

Toxic Mold, 8 HASTINGS W.-NW. J. ENVTL. L. & POL'Y 73 (2001). Hastings West-Northwest Journal of Environmental Law & Policy, U.C. Hastings College of the Law, 200 McAllister St., San Francisco, CA 94102.

Tod I. Zuckerman, Intellectual Property Insurance Coverage Disputes: A Primer and a State-by-state Survey of Cases, 29 LINCOLN L. REV. 1 (2001). Lincoln Law Review, One North First St., San Jose, CA 95113.

Note (W. Devin Resides), Holding HMOs Liable in the New Millennium: New Theories with an Old Twist, 27 OKLA. CITY U. L. REV. 419 (2002). Oklahoma City University School of Law Law Review, 2501 N. Blackwelder, Oklahoma City, OK 73106.

Comment (D. Chris Harkins), The Writing Is on the Wall . . . and Inside It: The Recent Explosion of Toxic Mold Litigation and the Insurance Industry Response, 33 TEX. TECH L. REV. 1101 (2002). Texas Tech School of Law Law Review, 1802 Hartford, Lubbock, TX 79409.

J. Stephen Zielezienski & Catherine I. Paolino, Insurance Privacy after Gramm-Leach-Bliley—Old Concerns, New Protections, Future Challenges, 37 TORT & INS. L.J. 1139 (2002). Tort and Insurance Law Journal, American Bar Association, Box 10892, Chicago, IL 60610-0892.

Louis J. Papa & Anthony Basile, No-Fault Insurance Fraud: An Overview, 17 TOURO L. REV. 611 (2001). Touro Law Review, Jacob D. Fuchsberg Law Center, Room 201, 300 Nassau Road, Huntington, NY 11743.

Jeffrey Thomas, Insurance Implications of September 11 and Possible Responses, 34 URB. LAW. 727 (2002). *Urban Lawyer*, University of Missouri—Kansas City, 5100 Rockhill Road, Kansas City, MO 64110-2499.

Procedure

William B. Rubenstein, The Concept of Equality in Civil Procedure, 23 CARDOZO L. REV. 1865 (2002). Cardozo Law Review, 55 Fifth Avenue, New York, NY 10003-4391.

Kevin M. Clermont & Theodore Eisenberg, Litigation Realities, 88 CORNELL L. REV. 119 (2002). Cornell Law Review, Cornell Law School, Myron Taylor Hall, Ithaca, NY 14853-4901.

Geoffrey Parmer, What "Erin Brockovich" Failed to Tell You about the Realities of Class Action Litigation, DISP. RESOL. J., May-July 2002, at 19 (2002). Dispute Resolution Journal, American Arbitration Association, 335 Madison Ave., New York, N.Y. 10017-4605.

Robert M. Brava-Partain, Due Process, Rule 23 and Hybrid Classes: A Practical Solution, 53 HASTINGS L.J. 1359 (2002). Hastings Law Journal, 200 McAllister St., San Francisco, CA 94102.

Edward H. Cooper, Simplified Rules of Federal Procedure? 100 MICH. L. REV. 1794 (2002). Michigan Law Review, Hutchins Hall, 625 S. State St., Ann Arbor, MI 48109-1215.

Jack B. Weinstein, A Survey of Changes in United States Litigation, 76 ST. JOHN'S L. REV. 379 (2002). St. John's Law Review, St. John's University School of Law, 8000 Utopia Parkway, Jamaica, NY 11439.

Note (Mary C. Cavanagh), Interpreting Rule 60(B)(6) of the Federal Rules of Civil Procedure: Limitations on Relief from Judgments for "Any Other Reason," 7 SUFFOLK J. TRIAL & APP. ADVOC. 127 (2002). Suffolk Journal of Trial and Appellate Advocacy, Suffolk University Law School, 120 Tremont St., Boston, MA 02108.

Richard H. Dreyfuss, Class Action Judgment Enforcement in Italy: Procedural "Due Process" Requirements, 10 TULANE J.

INT'L & COMP. L. 5 (2002). Tulane Journal of International and Comparative Law, Tulane University Law School, 6329 Freret St., New Orleans, LA 70118-2631.

Laurens Walker, A Model Plan to Resolve Federal Class Action Cases by Jury Trial, 88 VA. L. REV. 405 (2002). Virginia Law Review, 580 Massie Road, Charlottesville, VA 22903-1789.

Products Liability

David W. Prince & Paul H. Rubin, The Effects of Product Liability Litigation on the Value of Firms, 4 AM. L. & ECON. REV. 44 (2002). American Law and Economics Review, Box 208245, 127 Wall St., New Haven, CT 06520.

James A. Henderson Jr., Echoes of Enterprise Liability in Product Design and Marketing Litigation, 87 CORNELL L. REV. 958 (2002). Cornell Law Review, Cornell Law School, Myron Taylor Hall, Ithaca, NY 14853-4901.

Andrew E. Falsetti, Fluoxetine-induced Suicidal Ideation: An Examination of the Medical Literature, Case Law and the Legal Liability of Drug Manufacturers, 57 FOOD & DRUG L.J. 273 (2002). Food and Drug Law Journal, Food and Drug Law Institute, 1000 Vermont Ave. N.W., Suite 200, Washington, DC 20005.

Note (Mark D. Shifton), The Restatement (Third) of Torts: Products Liability—The ALI's Cure for Prescription Drug Design Liability, 29 FORDHAM URB. L.J. 2343 (2002). Fordham Urban Law Journal, 140 W. 62d Street, New York, NY 10023.

Casenote (Sheila J. Baran), "Good Cause" Wins the Battle, But Will Protective Orders Survive the Product Liability War? 53 MERCER L. REV. 1675 (2002). Mercer Law Review, Walter F. George School of Law, Mercer University, Macon, GA 31207.

Richard L. Cupp Jr. & Danielle Polage, The Rhetoric of Strict Products Liability Versus Negligence: An Empirical Analysis, 77 N.Y.U. L. REV. 874 (2002). New York University Law Review, 110 W. Third St., New York, NY 10012.

Note (Katrina R. Atkins), Defining the Duty of Gun Manufacturers in Hamilton v. Beretta U.S.A., 29 N. KY. L. REV. 849 (2002). Northern Kentucky Law Review, Northern Kentucky University, Salmon P. Chase College of Law, Nunn Hall Room 319, Highland Heights, KY 41099.

David A. Fischer, Product Liability: A Commentary on the Liability of Suppliers of Component Parts and Raw Materials, 53 S.C. L. REV. 1137 (2002). South Carolina Law Review, University of South Carolina School of Law, Columbia, SC 29208.

Note (Gary Zhao), Chinese Product Liability Law: Can China Build Another Great Wall to Protect Its Consumers? 1 WASH. U. GLOBAL STUD. L. REV. 581 (2002). Washington University Global Studies Law Review, Washington University School of Law, Campus Box 1120, One Brookings Drive, St. Louis, MO 63130-4899.

Professional Responsibility

Steven Shavell, Law Versus Morality as Regulators of Conduct, 4 AM. L. & ECON. REV. 227 (2002). American Law and Economics Review, Box 208245, 127 Wall St., New Haven, CT 06520.

Laurel S. Terry, MDPs, "Spinning" and Wouters v. NOVA, 52 CASE W. RES. L. REV. 867 (2002). Case Western Reserve Law Review, CWRU School of Law, 11075 E. Boulevard, Cleveland, OH 44106.

William H. Simon, The Belated Decline of Literalism in Professional Responsibility Doctrine: Soft Deception and the Rule of Law, 70 FORDHAM L. REV. 1881 (2002). Fordham Law Review, 140 W. 62d St., New York, NY 10023.

Margaret Colgate Love, The Revised ABA Model Rules of Professional Conduct: Summary of the Work of Ethics 2000, 15 GEO. J. LEGAL ETHICS 441 (2002).

Valerie Breslin & Jeff Dooley, Whistle Blowing v. Confidentiality, 15 GEO. J. LEGAL ETHICS 719 (2002). Georgetown Journal of Legal Ethics, Georgetown University Law Center, 600 New Jersey Ave. N.W., Washington, DC 20001.

Fred C. Zacharias, What Lawyers Do When Nobody's Watching: Legal Advertising as a Case Study of the Impact of Underenforced Professional Rules, 87 IOWA L. REV. 971 (2002). Iowa Law Review, University of Iowa College of Law, Boyd Law Building, Melrose and Byington, Iowa City, IA 52242-1113.

Virginia H. Underwood & Richard H. Underwood, The Attorney-client and Work Product Privileges: The Case for Protecting Internal Investigations on the University Campus, 90 KY. L.J. 531 (2002). Kentucky Law Journal, University of Kentucky College of Law, Lexington, KY 40506-0048.

Casenote (Matthew G. Steinhilber), Excessive Focus on Mitigating Factors in Attorney Misconduct Case Fails to Preserve Public Confidence in the Legal Profession, 61 MD. L. REV. 482 (2002). Maryland Law Review, 515 W. Lombard St., Baltimore, MD 21201.

Tony Honore, The Necessary Connection Between Law and Morality, 22 OXFORD J. LEGAL STUD. 489 (2002). Oxford Journal of Legal Studies, Journals Department, Oxford University Press, Great Clarendon St., Oxford OX2 6DP, U.K.

Peter Eggenberger, License to Bill = License to Kill? Ethical Considerations on Lawyers' Fees (with a View to Switzerland), 20 PENN ST. INT'L L. REV. 505 (2002). Penn State International Law Review, Pennsylvania State University, 150 S. College St., Carlisle, PA 17013.

Susan Saab Fortney & Jett Hanna, Fortifying a Law Firm's Ethical Infrastructure: Avoiding Legal Malpractice Claims based on Conflicts of Interest, 33 ST. MARY'S L.J. 669 (2002). St. Mary's Law Journal, One Camino Santa Maria, San Antonio, TX 78228-8604.

Barry R. Temkin, Can Negligent Referral to Another Attorney Constitute Legal Malpractice? 17 TOURO L. REV. 639 (2001). Touro Law Review, Jacob D. Fuchsberg Law Center, Room 201, 300 Nassau Road, Huntington, NY 11743.

Sarah Stephens McNeal, Lawyers Doing Business with Their Clients: Identifying and Avoiding Legal and Ethical Dangers: A Report of the Task Force on the Independent Lawyer, 3 TRANSACTIONS: TENN. J. BUS. L. 47 (2002). Transactions: Tennessee Journal of Business Law, University of Tennessee College of Law, 1505 W. Cumberland Ave., Knoxville, TN 37996-1810.

Sean J. Griffith, Ethical Rules and Collective Action: An Economic Analysis of Legal Ethics, 63 U. PITT. L. REV. 347 (2002). University of Pittsburgh Law Review, 3900 Forbes Ave., Pittsburgh, PA 15260.

Sanford M. Stein & Jan M. Geht, Legal Ethics for Environmental Lawyers: Real Problems, New Challenges and Old Values, 26 WM. & MARY ENVTL. L. & POL'Y REV. 729 (2002). William and Mary Environmental Law and Policy Review, College of William and Mary, Box 8795, Williamsburg, VA 23187.

Torts

Eric Helland & Alexander Tabarrok, The Effect of Electoral Institutions on Tort Awards, 4 AM. L. & ECON. REV. 341 (2002). American Law and Economics Review, Box 208245, 127 Wall St., New Haven, CT 06520.

Michael L. Rustad & Thomas H. Koenig, Taming the Tort Monster: The Ameri-

can Civil Justice System as a Battleground of Social Theory, 68 BROOKLYN L. REV. 1 (2002). Brooklyn Law Review, Brooklyn Law School, 250 Joralemon St., Brooklyn, NY 11201.

Note (Ryan M. Springer), On Causation and Comparison: Medical Malpractice and other Professional Negligence after Steiner Corp. v. Johnson & Higgins, 16 BYU J. PUB. L. 355 (2002). BYU Journal of Public Law, J. Reuben Clark Law School, 460 JRCB, Brigham Young University, Provo, UT 84602-8000.

Patrick J. Kelley & Laurel A. Wendt, What Judges Tell Juries about Negligence: A Review of Pattern Jury Instructions, 77 CHI.-KENT L. REV. 587 (2002). Chicago-Kent Law Review, Chicago-Kent College of Law, 565 W. Adams St., Chicago, IL 60661-3691.

Michael D. Mirne, The Brawl at Wrigley: An Analysis of Tort Liability, 9 SPORTS LAW. J. 95 (2002). Sports Lawyers Journal, Tulane University School of Law, 6329 Freret St., New Orleans, LA 70118.

Danielle Conway-Jones, Factual Causation in Toxic Tort Litigation: A Philosophical View of Proof and Certainty in Uncertain Disciplines, 35 U. RICH. L. REV. 875 (2002). University of Richmond Law Review, T.C. Williams School of Law, Room 301, University of Richmond, Richmond, VA 23173.

Local Interest

California

Casenote (Tracey Angelopoulos), Pavlovich v. Superior Court: Spinning a World Wide Web for California Personal Jurisdiction, 39 SAN DIEGO L. REV. 1019 (2002). San Diego Law Review, University of San Diego School of Law, 5998 Alcala Park, San Diego, CA 92110.

Matthew J. Madalo, Ethics Year in Review, 42 SANTA CLARA L. REV. 1291 (2002). Santa Clara Law Review, Santa Clara University, Santa Clara, CA 95053.

Florida

Leonard Birdsong, The Residual Exception to the Hearsay Rule—Has It Been Abused—A Survey Since the 1997 Amendment, 26 NOVA L. REV. 59 (2001). Nova Law Review, Nova Southeastern University, 3305 College Ave., Fort Lauderdale, FL 33314.

Illinois

Casenote (Byron Christopher Williams), The Content of His Character: Hale v. Comm. on Character and Fitness of the Illinois Bar, 4 T.M. COOLEY J. PRAC. & CLINICAL L. 269 (2001). Thomas M. Cooley Journal of Practical and Clinical Law, Thomas M. Cooley Law School, 217 S. Capitol Ave., Lansing, MI 48933.

Indiana

Note (Gregory A. Bullman), A Right Without a Potent Remedy: Indiana's Bad Faith Insurance Doctrine Leaves Injured Third Parties Without Full Redress, 77 IND. L.J. 787 (2002). Indiana Law Journal, Indiana University School of Law, Law Building, Room 009, Bloomington, IN 47405-1001.

Jeffrey O. Cooper, The Continuing Complexity of Indiana Rule of Evidence 404(b), 35 IND. L. REV. 1415 (2002).

Joseph R. Alberts, Survey of Recent Developments in Indiana Product Liability Law, 35 IND. L. REV. 1427 (2002).

Charles M. Kidd, Survey of the Law of Professional Responsibility, 35 IND. L. REV. 1477 (2002).

Timothy C. Caress & Katherine Amy Lemon, Recent Developments in Indiana Tort Law, 35 IND. L. REV. 1583 (2002). Indiana Law Review, Indiana University School of Law—Indianapolis, 530 W. New York St., Indianapolis, IN 46202-3225.

Louisiana

Comment (Wendy Watrous), Lawyer or Loan Shark? Rule 1.8(E) of Louisiana's Rules of Professional Conduct Blurs the Line, 48 LOY. L. REV. 117 (2002). Loyola Law Review, Loyola University New Orleans School of Law, 7214 St. Charles Ave., Campus Box 901, New Orleans, LA 70118.

Michigan

Daniel P. Ryan, Michigan Rule of Evidence 702: Amend It or Leave It to Schanz? 19 T.M. COOLEY L. REV. 1 (2002). Thomas M. Cooley Journal of Practical and Clinical Law, Thomas M. Cooley Law School, 217 S. Capitol Ave., Lansing, MI 48933.

Missouri

Bobbi McAdoo & Art Hinshaw, The Challenge of Institutionalizing Alternative Dispute Resolution: Attorney Perspectives on the Effect of Rule 17 on Civil Litigation in Missouri, 67 MO. L. REV. 473 (2002). Missouri Law Review, University of Missouri—Columbia, 203 Hulston Hall, Columbia, MO 65211-4190.

Nevada

Note (Carl Tobias), Waiting for Daubert: The Nevada Supreme Court and the Admissibility of Expert Testimony, 2 NEV. L.J. 59 (2002).

Note (Brian Irvine), Intentional Infliction of Mental Distress in Nevada, 2 NEV. L.J. 158 (2002). Nevada Law Journal, 4505 Maryland Parkway, Box 451003, Las Vegas, NV 89154-1003.

New Jersey

Seymour Moskowitz, Rediscovering Discovery: State Procedural Rules and the Level Playing Field, 54 RUTGERS L. REV. 595 (2002). Rutgers Law Journal, 5th & Penn Sts., Suite 510, Camden, NJ 08102.

New York

Sha-Shana N.L. Crichton, Distinguishing Between Direct and Consequential Damages under New York Law in Breach of Service Contract Cases, 45 HOW. L.J. 597 (2002). Howard Law Journal, 2900 Van Ness St. N.W., Washington, DC 20008.

Joel Slawotsky, New York's Article 16 and Multiple Defendant Product Liability Litigation: A Time to Rethink the Impact of Bankrupt Shares on Judgment Molding, 76 ST. JOHN'S L. REV. 397 (2002). St. John's Law Review, St. John's University School of Law, 8000 Utopia Parkway, Jamaica, NY 11439.

Paul H. Aloe, Civil Practice, 52 SYRACUSE L. REV. 227 (2002).

Michael J. Hutter, Evidence, 52 SYRACUSE L. REV. 397 (2002).

Thomas F. Segalla & Richard J. Cohen, Insurance Law, 52 SYRACUSE L. REV. 449 (2002).

Steven Wechsler, Professional Responsibility, 52 SYRACUSE L. REV. 563 (2002).

Scott L. Haworth, Torts, 52 SYRACUSE L. REV. 677 (2002). Syracuse Law Review, Syracuse University College of Law, Syracuse, NY 13244-1030.

Pennsylvania

Seth William Goren, A Pothole on the Road to Recovery: Reliance and Private Class Actions under Pennsylvania's Unfair Trade Practices and Consumer Protection Law, 107 DICK. L. REV. 1 (2002). Dickinson Law Review, Dickinson School of Law, 150 S. College St., Carlisle, PA 17013.

Texas

Mark L. Kincaid & Trevor A. Taylor, Annual Survey of Texas Insurance Law 2002, 6 J. TEX. CONSUMER L. 2 (2002). Journal of Texas Consumer Law, University of Houston Law Center, 100 Law Center Houston, TX 77204-6060.

Steve McConnico & Robyn Bigelow, Summary of Recent Developments in Texas Legal Malpractice Law, 33 ST. MARY'S L.J. 607 (2002).

Broadus A. Spivey, Ethics: Lawyering and Professionalism, 33 ST. MARY'S L.J. 721 (2002). St. Mary's Law Journal, One Camino Santa Maria, San Antonio, TX 78228-8604.

Appellate Practice Group of Locke, Liddell & Sapp, Recurring Issues in Consumer and Business Class Action Litigation in Texas, 33 TEX. TECH L. REV. 971 (2002). Texas Tech School of Law Law Review, 1802 Hartford, Lubbock, TX 79409.

West Virginia

Student Article (Sean R. Levine), Spoliation of Evidence in West Virginia: Do Too Many Torts Spoliate the Broth? 104 W. VA. L. REV. 419 (2002). West Virginia Law Review, Box 6130, Morgantown, WV 26506-6130.

Correction

An error occurred in the U.S. Postal Service Statement of Ownership, Management and Circulation, which appeared on page 400 of the October 2002 issue of *Defense Counsel Journal*. The figure in Paragraph 15(h), actual nearest filing date, should be 786.

About the IADC

The International Association of Defense Counsel is the oldest and most prestigious international association of attorneys representing corporations and insurers. Its activities benefit not only the approximately 2,400 invitation-only, peer-reviewed members and their clients through networking, education and professional opportunities, but also the civil justice system and the legal profession. The IADC takes a leadership role in many areas of legal reform and professional development.

Founded in 1920, IADC's membership comprises the world's leading corporate and insurance attorneys, partners in large and small law firms, senior counsel in corporate law departments, and corporate and insurance executives. They engage in the practice and management of law involving the defense, prosecution and resolution of claims affecting the interests of corporations and insurers. The Association maintains a comprehensive list of publications and training programs, including the quarterly Defense Counsel Journal. It holds annual and midyear meetings and sponsors the IADC Trial Academy, the IADC Corporate Counsel College, and the IADC Fidelity and Surety Trial Practice Program, each held annually. The IADC founded the Defense Research Institute and co-founded Lawyers for Civil Justice.