The Federal Lawyer

September 2007 Volume 54 Number Eight

Columns

Departments

Book Reviews

Information Privacy Law

The Federal Lawyer (ISSN: 1080-675X) is published 10 times per year, monthly, except for March/April and Nov./Dec. when it is bimonthly, by the Federal Bar Association, 2011 Crystal Drive, Ste. 400, Arlington, VA 22202; Tel. (703) 682-7000, Fax (703) 682-7001, E-mail: tfl@fedbar.org. Editorial Policy: The views published in *The Federal Lawyer* do not necessarily imply approval by the FBA or any agency or firm with which the authors are associated. All copyrights are held by the FBA unless otherwise noted by the author. The appearance of advertisements and new product or service information in *The Federal Lawyer* does not constitute an endorsement of such products or services by the FBA. Manuscripts: *The Federal Lawyer* accepts unsolicited manuscripts, which, if accepted for publication, are subject to editing. Manuscripts must be original and should appeal to a diverse audience. Visit www.fedbar.org/guidelines.html for writer's guidelines. Subscription Rates: $14 of each member's dues are applied toward a subscription. Nonmember domestic subscriptions are $35 each per year; foreign subscriptions are $45 each per year. All subscription prices include postage. Single copies are $5. Periodical postage paid in Arlington, Va., and at additional mailing offices. POSTMASTER, send changes of address to: *The Federal Lawyer*, The Federal Bar Association, 2011 Crystal Drive, Ste. 400, Arlington, VA 22202.

The Federal Bar Association | Mission Statement

The mission of the Association is to advance the science of jurisprudence and to promote the welfare, interests, education, and professional growth and development of the members of the Federal legal profession.

The Federal Bar Association
2011 Crystal Drive, Ste. 400 | Arlington, VA 22202 | Telephone (703) 682-7000 | 24-Hour Fax (703) 682-7001 | E-mail: fba@fedbar.org

WILLIAM N. LAFORGE

The Page Turns: Building a Tradition of Excellence

With this last column, I am happy to report to our membership that I leave office with an even greater sense of optimism and expectation for a bright future for the FBA than I had when I began my term of office a year ago. In fact, I would go so far as to say that we are well on our way to building a tradition of excellence.

The proverbial page has turned. My successor, Jim Richardson, has been installed, and, as a result of this year's elections, the composition of the FBA Board of Directors remains the same. It is a pleasure to pass the gavel to Jim, as he assumes the privilege of presiding over a group of outstanding directors and an association that is on the move.

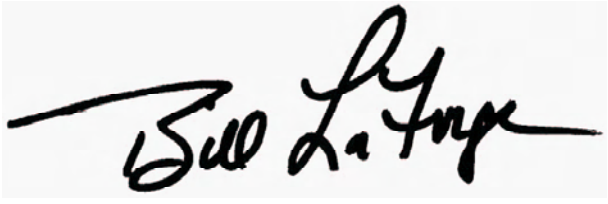
Paramount during my year in office has been the ongoing effort to put our organizational house in order under the new governance structure. I am pleased to report that this priority goal has been accomplished for the most part, largely thanks to the valuable contributions of scores of volunteer leaders and the association's staff, who have committed themselves to ensuring a smooth transition. Our new Board of Directors is up and running on all cylinders. There are still processes to be completed, but, by and large, all systems are "go" for Jim and the new board to take the association to greater heights. I wish them every success in accomplishing the FBA's goals.

With the privilege of the president's pen, I have had the unique opportunity to write and opine about a variety of issues in this column during my term of office. From an outline of the year's goals, mini-treatises on judicial independence and government relations, a tribute to federal judges who are involved with the FBA, and some personal perspectives on the law—to the characteristics of the new and changing FBA, advice for law graduates and new lawyers, and commentaries on our chapters, leadership training, diversity, and members' perspectives—I have sought to run the gamut in commenting on issues that I consider timely and important for the association.

I complete my term as president at an exciting time for the FBA, but there is still much for all of us to do. With the outstanding work and report of the Task Force on the Future, so ably chaired by Rob Clark of the Utah Chapter, the association has in place a superb road map that can be used to move the association forward. In the months ahead, the Board of Directors will review the report and conclusions of the task force, formulate a plan of action, and communicate the results to the association at all levels, with an eye toward implementing new programs and policies that will provide a foundation of strength on which a productive and successful future can be built. I consider the good work of the Task Force on the Future and the application of its guidelines to be major steps in creating a tradition of excellence for the Federal Bar Association.

I extend my sincerest thanks to Executive Director Jack Lockridge and his very capable staff for all they have done to make this year the success it has been. The FBA can be very proud of Jack and the outstanding job he does each day in representing our best interests and in managing the association. I am very grateful to Dan McDonald, to whom I presented the President's Award at the recent annual meeting, and the board of the Federal Bar Building Corporation for their hard work and devotion to the association throughout the challenge of selling the former headquarters facility and locating a new home for the FBA. And I thank our outstanding inaugural Board of Directors and all our volunteer leaders around the country for their inspiration, hard work, and commitment to the FBA. All these special individuals and many more are the real reasons the FBA is on the right track to establishing a tradition of excellence.

The FBA is blessed with an outstanding talent pool that is set to guide an association that has not yet reached its full potential. Ours is a particularly bright future if we can capitalize on the foundation that has been put in place over the last several years to advance our interests and to ensure that the FBA remains a meaningful and valuable experience for its members. It has been a privilege for me to serve the FBA and its membership as national president. **TFL**



NATHAN BROOKS

Information Privacy

IT HAS BEEN well over 100 years since Samuel Warren and Louis Brandeis drew the outlines of privacy law for the century that followed. What they termed "the right to be let alone" (borrowed from a 19th-century torts treatise) became the guidepost for the evolution of the field over the next century. Whether discussing illegal searches or penumbras of privacy, judges always seemed to focus their analyses (whether they admitted it or not) on the simple but powerful idea that all of us exercise a certain sovereignty over our persons—an "inviolate personality"—that must be respected.

Since the years following World War II, however, a powerful undercurrent of thought has evolved with respect to privacy focused on personal information. The second half of the 20th century saw technological advances that made it increasingly possible to monitor and track persons as a result of the amazing amounts of personal identifying data that could be stored in ever more efficient ways. Governments that had always wanted to keep tabs on their citizens now had the means to do so and, with the paranoia that attended the Cold War, had a harrowing sense of urgency.

As innovations in computer technology continued at an incredible pace, authors and commentators began to warn of a future in which governments could use personal data to track and control the masses. To many, the right to be let alone was taking on a meaning different from the one that Warren and Brandeis had in mind. The new understanding of "information privacy" held that information is power, and the increasing availability of personal data created a real danger that this power would be abused.

The Orwellian vision of the omnipresent government eye never materialized, but the debate over information privacy did not die. Of course, personal information has real business value, and in place of the over-the-top warnings that "Big Brother" would use our personal information to exert control came the more realistic call for regulation of the business of personal information.

The rise of commerce over the Internet has exponentially increased the value of personal information. The business owner or banker identifies the customer not by his or her face but rather by the person's Social Security number or credit card number. Such information is often easy to steal and even easier to use. But personal data do not simply facilitate commerce; they also include information about criminal backgrounds and credit histories that employers, lenders, and others use in assessing the risks associated with their business decisions. Thus, in many instances, the person who complains that the availability of personal data leads to identity theft is the same person who requests a background check on the babysitter to ensure the safety of his or her children. The central question, then, is not how to prevent the collection and use of personal data completely, but rather how to make sure this information is used and secured properly.

The law has been slow to catch up with these concerns, and in this issue we not only examine some of the methods available for addressing these concerns but also identify a few of the difficulties that are lurking around the corner. Internet Protocol Version 6, for example, is set to greatly expand the amount of information the Internet can support, and yet relatively few people have even heard of the protocol, much less understand its importance.

The current legal framework in America is a patchwork solution at best, barely (if at all) able to curtail the rise of identity theft. Congress has been unable to pass comprehensive legislation designed to protect data, and the somewhat outdated Fair Credit Reporting Act remains one of the major federal laws related to information privacy. The U.S. Supreme Court recently had a chance to interpret this statute and, as discussed in this issue, the justices offered a revealing glimpse into their collective perspective of the act.

Advocates of legislation safeguarding the privacy of personal information can also look to the Gramm-Leach-Bliley Act, also imperfect, which can be enforced through private litigation or, somewhat controversially, enforced by the Federal Trade Commission. In this issue, two attorneys on the front lines of the battle over this act provide analyses of these separate enforcement mechanisms.

It seems clear that the federal government should enact comprehensive legislation designed to protect personal data, because in the absence of such a regime the states have enacted their own very different statutes. In searching for answers as to what a

federal program might look like, some commentators turn to Europe, where the horrors of the calculated mass murder that was the Holocaust loom large in the public consciousness, and information privacy is seen as a fundamental human right. An article in this issue examines the data protection regime implemented by the European Union to see if the European experiment offers lessons for the United States.

Many questions raised in this issue are familiar to readers of this journal, for example—

- How do we balance business needs with concerns over consumer protection concerns?
- In what persons or agencies should enforcement authority reside?

In reality, even though these questions may seem familiar, within the context of information privacy, the answers should be anything but. Information technology is already moving much faster than our legislators and regulators can respond to the advances, and those on the horizon threaten to put us even further behind.

In distinguishing information privacy from the original concept of the right to be let alone, Julie Cohen, author and Georgetown Law School professor of information privacy law, offered the following valuable advice: "The universe of all information about all record-generating behaviors generates a 'picture' that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it. In such a world, we should all be cautious." **TFL**

Nathan Brooks serves as general counsel at U.S. ISS Agency, a security consulting firm in Charlotte, N.C., and is a member of the FBA Editorial Board.

Editorial Policy

The Federal Lawyer is the magazine of the Federal Bar Association. It serves the needs of the association and its members, as well as those of the legal profession as a whole and the public.

The Federal Lawyer is edited by members of its editorial board, who are all members of the Federal Bar Association. Editorial and publication decisions are based on the board's judgment.

The views expressed in *The Federal Lawyer* are those of the authors and do not necessarily reflect the views of the association or of the editorial board. Articles and letters to the editor in response are welcome.

D.C. Circuit

Capitol Hill

The Capitol Hill Chapter has sponsored a wide variety of events this year. The highlight was the chapter's luncheon program held at the U.S. Supreme Court on May 22, an annual event the chapter has hosted for more than 30 years. This year's keynote speaker was Chief Justice of the United States John G. Roberts Jr., who shared his insights on issues ranging from judicial pay and separation of powers to contributions of the early Chief Justices. The Chief Justice offered his remarks and responded to questions from the FBA member audience—including FBA President William N. LaForge and FBA President-elect James S. Richardson Sr.—following a formal lunch in the Supreme Court's West Conference Room. Chapter President Susan D. Sawtelle introduced Chief Justice Roberts.

This year's chapter speaker programs have featured U.S. Sen. Benjamin Cardin (D-Md.); James Duff, director of the Administrative Office of the U.S. Courts; Alan Hantman, architect of the Capitol; Joan Winship, executive director, and Anne Goldstein, human rights education director, International Association of Women Judges; Jan Crawford Greenburg, ABC News legal correspondent and author of *Supreme Conflict: The Inside Story of the Struggle for Control of the U.S. Supreme Court*; and constitutional lawyer David Stewart, author of *The Summer of 1787: The Men Who Invented the Constitution*.

The chapter has also helped organize and has participated in a number of important community and cultural events this year. These have included a Feb. 21 tour of the site of the new Capitol Visitors Center—now under construction below the East Capitol grounds—led by staff members of the architect of the Capitol. The center will welcome visitors in a secure public environment and is the largest project in the Capitol's 212-year history. The Visitors Center will be approximately three-quarters the size of the Capitol itself.

And stretching their muscles for a good cause, members of the Capitol Hill and Pentagon Chapters, including FBA President Bill LaForge, fielded Team FBA on June 9 at the Lawyers Have Heart 10K Run & Walk. The D.C. Circuit-based team, organized by Capitol Hill Chapter Past President and D.C. Circuit Vice President James Scott, participated in the event, which benefits the American Heart Association and the American Stroke Association. **TFL**

Team FBA at the Lawyers Have Heart 10K Run & Walk—(l to r) Warren Burke, Capitol Hill Chapter immediate past president and member of the FBA Board of Directors; FBA President Bill LaForge; two friends of the team; T.J. Halstead, Capitol Hill Chapter treasurer; Kathleen Duignan, Pentagon Chapter president; James Scott, Capitol Hill Chapter past president and D.C. Circuit vice president; Susan Sawtelle, Capitol Hill Chapter president; Paul Vamvas, Capitol Hill Chapter vice president; Jeffrey Good, Pentagon Chapter 1st vice president.

Chapter Exchange is compiled by Anne Daugherty, FBA manager of chapters and circuits. Send your chapter information to adaugherty@fedbar.org or Chapter Exchange, FBA, 2011 Crystal Drive, Ste. 400, Arlington, VA 22202.

Capitol Hill Chapter: At the annual luncheon program held at the U.S. Supreme Court—(left photo, l to r) T.J. Halstead, chapter treasurer; Warren Burke, immediate past chapter president and member of the FBA Board of Directors; Judge Bruce Kasold, former chapter president; Susan D. Sawtelle, chapter president; Chief Justice John G. Roberts Jr.; Adam Bramwell, chapter president-elect; and Richard Litsey, chapter secretary; (right photo) Chief Justice Roberts and FBA President William N. LaForge.

Ninth Annual Washington, D.C. Indian Law Conference

Pragmatic Approach to Modern Indian Country Concerns

October 19, 2007
Westin Grand ▸ 2350 M Street N.W.

Schedule

9-11 a.m.	**Roundtable with Decision Makers: Indian Gaming, Indian Lands—How Do the Feds Make Decisions?**
11:15 a.m.–12:15 p.m.	**A New "Roberts Court" Jurisprudence for Native American Casess?**
12:30-1:30 p.m.	**Luncheon and Keynote Address: A Pragmatic Approach to Ethical Issues in Indian Country** Luncheon Speaker—Maylinn Smith, associate professor/director of Indian Law Clinic, University of Montana School of Law
2:15–3:30 p.m.	**Case Study: Tribal Best Practices—Innovative Ways of Meeting Tribal Goals in Cooperation with the Federal Government: Standing Rock Sioux Tribe Takes Charge of Its Roads and Infrastructure**
3:45–5 p.m.	**Protecting Tribal Rights Through Environmental Regulation**

Focusing on the practical concerns facing Indian Country, this year's mid-year conference provides practitioners an opportunity to zero in on the most pressing issues facing Indian Country today, including: how/why Indian lands determinations are made; an advanced discussion of the Supreme Court docket with leading lawyers in the field; a segment discussing real ethical quandaries faced by tribal lawyers; and "tribal best practices" related to tribal transportation and environmental programs.

The conference's intimate setting gives participants an opportunity to interact with actual decision makers and leading innovators in the field of Indian law. Taking a page from the approach made famous by law professor Arthur Miller, the moderator of the first panel discussion will seek to: create lively interaction among the panel members, make the topic of Indian lands and Indian gaming come to life using hypothetical facts and scenarios and create an environment where opposing points of view can be challenged in a way that's respectful, thought-provoking, enlightening and, with some luck, entertaining.

Tribal leaders, advocates, and professionals interested in the field of Indian law are encouraged to join us for a day of dynamic review of pressing issues facing tribal governments today.

Sponsored By▸ Federal Bar Association Indian Law Section ▸ National Native American Bar Association ▸ Native American Bar Association of Washington, D.C.

Washington, D.C. Indian Law Conference ▸ Registration Form

Return to: D.C. Indian Law Conference, FBA, 2011 Crystal Drive, Suite 400, Arlington, VA 22202 or fax (703) 682-7001.

First Name M.I. Last Name

Firm/Agency

Street

City/State/Zip

Phone

Fax

E-mail

Check Appropriate Option

❑ $110 Law Student ❑ $230 FBA/NABA Member/Govn't Employee
❑ $345 Nonmember
❑ I would like to apply for membership in the FBA and pay the FBA membership fee. (Apply at www.fedbar.org.)

❑ I would like information on joining NABA.
CLE Write in state from which you need credit: _____

Method of Payment Payment must accompany registration.
❑ American Express ❑ Diners Club ❑ Mastercard
❑ Check (payable to FBA) ❑ Govt PO ❑ Visa

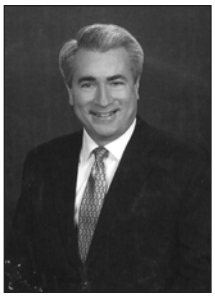
Card# _____ Exp. Date: _____

Cardholder Signature

BRUCE MOYER

Federal Bar Association 2007–2008 Issues Agenda

The Issues Agenda is the annual list of policy and legislative priorities to which the Federal Bar Association commits the attention and resources of its government relations program. The agenda is revised each year, addressing topical congressional and executive branch policy issues underlying the federal legal system and federal jurisprudence. Drafted by the Government Relations Committee with input from members, chapters, sections, and divisions, the Issues Agenda for 2007–2008—as reproduced below—was approved by the FBA Board of Directors at its July 21 meeting. The foremost change over the 2006–2007 agenda lies in the addition of FBA support for the restoration of criminal jurisdiction to Indian tribal courts, in accordance with federal, state, and tribal law, over non-Indian offenders in cases of domestic and family violence.



Legislative Issues To Be Actively Pursued

- Support the federal judiciary consistent with and in implementation of resolutions previously adopted by the Federal Bar Association, including support for:
  - — Adequate funding for the general and continuing operations of the federal courts, including an equitable level of rent and facilities expense consistent with actual costs, budgetary constraints, staffing needs, and security considerations, to permit the courts to fulfill their constitutional and statutory responsibilities;
  - — Equitable compensation and regular periodic adjustments for the federal judiciary as well as senior officials of the Executive Branch and Members of Congress, to promote the recruitment and retention of the highest quality public servants;
  - — Authorization and establishment of additional permanent and temporary federal judgeships, including bankruptcy judgeships, along with support personnel;
  - — Full funding of courthouse construction proposed by the U.S. Judicial Conference; and
  - — Adequate security measures to protect the federal judiciary, their families, and court personnel inside and outside the courthouse.
- Support the professionalism and stature of attorneys employed by the federal government, including:
  - — Enhancements to compensation packages, including pay and retirement benefits, to assist in recruitment and retention;
  - — Elevation of the grade of Judge Advocate Generals for the Army, Navy, and Air Force from two to three stars to ensure that military commanders have the benefit of independent legal advice from experienced military counsel;
  - — Expansion, consistent with applicable conflict of interest laws, of policies encouraging full participation in professional organizations and pro bono legal activities, including approval for use of administrative leave;
  - — Enhanced federal funding for participation in continuing legal education and training programs, including paid tuition and administrative leave; and
  - — Establishment of programs for student loan deferral and repayment assistance for all federal attorneys, including federal law clerks, federal defenders, and judge advocates of the Armed Forces, in support of recruitment and retention efforts.
- Support efforts to advance fairness and consistency in federal sentencing, while preserving judicial independence and discretion to deal with the particular circumstances of individual cases.
- Encourage and contribute to a discussion of the competing considerations in the nation's war against terror between the protection of civil liberties and the interests of national security.
- Support congressional funding to permit an increase in compensation rates for Criminal Justice Act panel attorneys, consistent with and in implementation of resolutions previously adopted by the FBA.
- Support the administrative judiciary, through the establishment of an Administrative Law Judge Conference, responsible for the testing, selection, and appointment of federal administrative law judges, as well as appropriate action by the Congress and the Executive Branch to preserve in future statutes the uniformity of process and qualifications of presiding officers contemplated by the Administrative Procedure Act.
- Support efforts to assure the continued use and independence of administrative law judges in the adjudication of Medicare benefit appeals.
- Support efforts by the Social Security Administration to take appropriate steps to ensure the security of its administrative law judges and all others who participate in its proceedings.

- Support the aims of the Indian Child Welfare Act to protect American Indian and Alaska Native families by recognizing the importance of tribal authority, culture, and tradition in decision-making for children subject to the Act.
- Support the restoration of criminal jurisdiction to Indian tribal courts, in accordance with federal, state, and tribal law, over non-Indian offenders in cases of domestic and family violence.
- Urge Congress to specify when military commissions may be used, what principles of law shall be applied to trial and sentencing by military commissions, and what rights shall be guaranteed to the accused.

Legislative Issues To Be Monitored

- Support the federal judiciary consistent with and in implementation of resolutions previously adopted by the Federal Bar Association, including support for:
  - — Development of strategies to reduce the time required to fill federal judicial vacancies; and
  - — Expansion of and enhanced federal funding for continuing legal education and training programs for the federal judiciary.
- Reaffirm the importance of the independence of the judiciary, recognizing that judicial decisions are not immune from scrutiny, but are to be made solely on the basis of the law.
- Advocate strict scrutiny of legislation proposing to grant original jurisdiction to federal authorities over crimes traditionally reserved for state and local prosecution.
- Oppose the division of the Ninth Circuit Court of Appeals, consistent with its capacity to effectively and efficiently render justice.
- Encourage and contribute to a discussion of the competing considerations vis-à-vis proposed legislation that would authorize federal judges, in their discretion, to permit photographing, electronic recording, broadcasting, and televising of federal court proceedings in appropriate circumstances.
- Address proposals to amend the Uniform Code of Military Justice and to make changes to the military justice system.
- Oppose proposed "user fees" in Social Security and SSI cases, consistent with and in implementation of resolutions previously adopted by the FBA.
- Address efforts by the Social Security Administration to reorganize its disability adjudication programs. **TFL**

Bruce Moyer is government relations counsel for the FBA.

MICHAEL J. TONSING

Federal Court Hearings on Your MP3 Player? Dude!

So, you're jogging on your favorite trail in suburban Omaha, the sun's coming up, the fields are a dewy emerald green, and you are listening on your headphones—for the 12th time—to your new favorite judge explaining to your high-density opposing counsel why your brilliant argument about pseudo-causality blew his socks off.

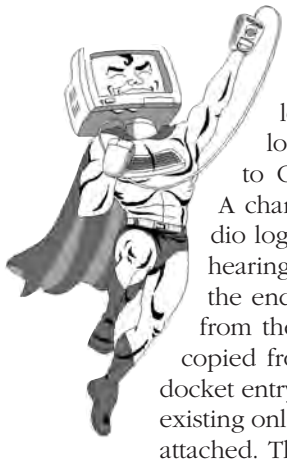
Dude! Forget music. This is why the iPod™ and the MP3 player were invented! Pseudo-causality rules! Fantasy? Nope.

Digital Audio in Trial Courts

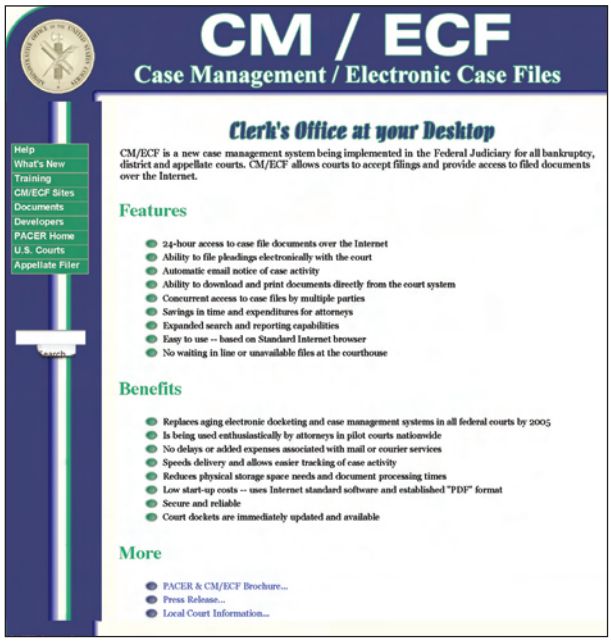
Two federal trial courts have already instituted a pilot project that makes digital audio recordings of courtroom proceedings publicly available in Cyberia. They can be downloaded from the court's official site, forwarded to clients, and archived in your hard drive's Hall of Fame library of personal best arguments.

Nebraska's district court and the Bankruptcy Court for the Eastern District of North Carolina are making selected digital audio files available in the same way that written files have already been available on the Internet.

All kidding aside, this new form of transcripts may prove to be very attractive to both lawyers and their clients. We'll soon see. By the time you read this column, Nebraska and North Carolina's Eastern District will have been joined by three other courts (the U.S. District Court for the Eastern District of Pennsylvania, the U.S. Bankruptcy Court for the District of Maine, and the U.S. Bankruptcy Court for the Northern District of Alabama).



Selected audio files from these five trial-level courts are can be accessed and downloaded as MP3s through the Public Access to Court Electronic Records (PACER) system. A chambers module interfaces with a digital audio log sheet that permits a judge to select which hearings he or she would like to make available at the end of each court day. The digital audio files from the selected hearings are then automatically copied from the court's digital audio system and a docket entry with a speaker icon is made in the court's existing online docketing system. The audio file is then attached. The Administrative Office of the U.S. Courts is providing model procedures that presiding judges in districts in the pilot program may voluntarily use to inform lawyers and parties to the litigation of the potential of having the audio recording of their hearing made available via PACER.



As you probably already know, PACER is the judiciary's central processing unit for electronic access to U.S. district, bankruptcy, and appellate court records. More than 700,000 Cyberian cognoscenti already use PACER to access electronic docket and case information from these federal courts across the country.

PACER, in turn, now ties to the federal courts' Case Management and Electronic Case Files system (CM/ECF). Dubbed the "Clerk's Office at Your Desktop," CM/ECF already allows federal courts to maintain case documents in electronic form. And, it gives each court the option of permitting case documents—pleadings, motions, petitions—to be filed with that court over the Internet. (If you need to learn more about CM/ECF itself, go to pacer.psc.uscourts.gov/cmecf/index.html.)

The next leap was tying CM/ECF to actual digital audio recordings of hearings. Mission accomplished!

Digital audio recording is already used in most bankruptcy courts and in many district courts (where magistrate judges account for most of the usage), replacing certified shorthand reporters. At last count, 37 of the nation's 642 active district court judges now use digital recording in their proceedings. In those trial courts using this technology, computer disks of hearings have been available for a fee of $26 for some time now, but prospective purchasers have had to trek to the local clerk of court's office to pay up.

During the five-court pilot project under way, access to audio files is available over the Internet at a bargain price: eight cents for accessing the docket sheet and another eight cents for the audio file itself. (At this price, it is almost as good as the old Napster!)

At its June 2008 meeting, the Judicial Conference Committee on Court Administration and Case Management, headed by Judge John R. Tunheim of the U. S. District Court for the District of Minnesota, will be provided with an evaluation of the pilot project and will decide its fate. If this noble experiment in gaining access to digital audio recordings becomes permanent, the Administrative Office will determine the appropriate fee later.

In the meantime, more information about obtaining trial court audio files through the pilot project can be found at a number of individual federal court Web sites. You may want to start with the official press release that recently announced the launch and was issued by the Administrative Office of the U.S. Courts, at www.uscourts.gov/Press_Releases/digialaudio080607.html.

More hands-on information for those who want to see how the process actually works is provided in a short video that is viewable through the Web sites of courts participating in the pilot project. This video, though a trifle sterile, methodically and expertly walks you through the rather magical process of downloading an audio file from a court's electronic docket. Try www.nceb.uscourts.gov and www.ned.uscourts.gov, and you'll get all the help you need to make you a true maestro of audio transcript downloading.

Appellate Audio, Too!

Meanwhile, the Seventh Circuit is the first federal court of appeals to make "RSS feeds" of audio recordings of oral arguments available "in bulk" from its Web site—www.ca7.uscourts.gov/ca7_rss.htm. (RSS stands for really simple syndication.) Using the system is about as simple as clicking on a button. A user simply "subscribes" to a particular topic (called an RSS feed), and an RSS reader periodically checks to see if there are any new items that fit the subscription's profile. If there are new items, the RSS reader automatically notifies the user.

An RSS reader can be a stand-alone program or an extension of a standard browser. Some browsers—such as the current versions of Firefox™ and Safari™—have built-in RSS readers. If you're using a browser that doesn't currently support RSS, there are readers available on the Web. Some are free to download, others are available for purchase.

As the Seventh Circuit's Web site proudly announces, "Now the content you want can be delivered directly to you without cluttering your inbox with e-mail messages." In this instance, the uncluttered content can include the audio files for the circuit's latest oral arguments.

The ability to hear other arguments before making one's own cannot help but improve the quality of oral advocacy. The ability to hear the voice and the questioning technique of the panelists set for one's own case cannot help but improve one's preparation. And the ability to hear one's own argument after the fact and to share it with the client should also help improve advocacy for those of us who learn from experience.

What could be easier? The RSS approach results in audio files being made available and allowing the end user (that's you, dude) to remain fairly passive. The RSS reader does the heavy lifting. Even though most RSS feeds seek out text, the technology can also seek out podcasts (recordings of audio or video files that can be downloaded to an iPod or other portable MP3 player). That is the capability that the Seventh Circuit is utilizing so effectively and innovatively. The Seventh Circuit's Web site makes available an RSS feed of arguments as a standard audio MP3 podcast and as an iTunes optimized audio podcast. Just choose and click.

Innovation such as this is not new in the Seventh Circuit. Over a decade ago, it was the first federal circuit with an electronic bulletin board (a type of pre-Internet system that allowed users to exchange messages and read news over a telephone line). The Seventh Circuit also was the first to require attorneys to submit electronic briefs on disks as well as the first to make audio of arguments available online. With the addition of an RSS feed, audio recordings of Seventh Circuit oral arguments are now available the same day that they occur.

The Seventh Circuit appears to be in the lead once again, when it comes to the accessibility of oral arguments; but the circuit is not alone by any means. Most federal courts of appeals now make audio files of oral arguments publicly available. The Eighth Circuit and the Federal Circuit, for example, make audio files of oral arguments available in MP3 format. The Ninth Circuit posts audio files of arguments on its Web site. And the D.C., First, Second, Fourth, and Sixth Circuits will all provide audio files on a CD upon request.

Conclusion

OK. I've put you on your personal path to fame and glory. Now, it's time for you to shape up your dewy emerald green argument about pseudo-causality, dude. It'll be a million seller. See you next month in Cyberia. **TFL**

Michael J. Tonsing practices law in San Francisco. He is a member of the FBA editorial board and has served on the Executive Committee of the Law Practice Management and Technology Section of the State Bar of California. He also mentors less experienced litigators by serving as a "second chair" to their trials. See www.YourSecondChair.com. He can be reached at mtonsing@lawyer.com.

RAYMOND J. DOWD

Rights of Publicity: Elvis, Marilyn, and the Federal Courts

Why does Elvis Presley's estate control the lucrative rights to licensing photographs that contain Elvis's image and Marilyn Monroe's estate have no such rights? And how did it come about that federal courts have become a major forum for enforcing these seemingly inequitable laws?

America's athletes, politicians, experts, and celebrities make fortunes by endorsing products, services, and vacation destinations. In connection with this lucrative industry, federal courts are frequently called upon to interpret a type of intellectual property known as "rights of publicity." The right of publicity is an outgrowth of the right of privacy, but the two rights protect fundamentally different interests and must be analyzed separately. The right of privacy, which protects the right to an individual's self-esteem and dignity, ends at the person's death. The right of publicity, on the other hand, is an intellectual property right that protects the pecuniary right and interest in the commercial exploitation of a celebrity's identity. Because the right of publicity is a property right, rather than a dignitary right, it can extend beyond death and can be bought and sold.[1] Rights of publicity do not generally require evidence of consumer confusion.[2]

In some states, a right of publicity during an individual's life as well as after his or her death is recognized by statute. New York and Wisconsin have expressly re- jected a post-mortem right of publicity altogether. In still other states, the right of publicity itself and its extent is uncertain and has not been defined.[3] For example, a U.S. district court in Pennsylvania recently held that a user of a 13-second recording of a deceased announcer's voice required the permission of the announcer's estate. Rejecting the argument that the copyright laws preempt Pennsylvania's right of publicity laws, the court permitted a recovery since use of the voice was a "misappropriation of identity."[4] New York's statute dealing with the right of publicity confers the right to use an actor's image only within the state of New York so uses in Germany would not be prohibited.[5]

This patchwork of laws has created difficulty for federal courts. For example, in 2001, the Sixth Circuit found a right of publicity under Michigan law, even though no court in Michigan had expressly recognized such a right. The Sixth Circuit upheld an injunction enforceable only in those states recognizing a post-mortem right of publicity.[6] The Tenth Circuit recently permitted a case to proceed to a jury trial in which, after terminating an employee, the employer distributed promotional material with the name of the well-known employee who had been terminated.[7] The Illinois Right to Publicity Act enacted in 1999 prohibits using a person's name in a domain name or a metatag to sell pornography.[8]

The basic rule that all attorneys should know in tackling right of publicity questions is the following: If a client (even a nonprofit organization or a government agency) wishes to use a living person's image for purposes of trade or advertising, the client must get a written release. If the attorney is unsure about what constitutes trade or advertising, it is important to consult the case law, because the answers may vary and there are numerous gray areas.

Rights of publicity arise in contexts involving other legal rights. For example, a client may wish to use a copyrighted photograph in which a person's face appears. Therefore, the second basic rule to remember in dealing with rights of publicity is that your client may need permission from more than one person. Absent certain circumstances—known as "fair use," as described in 17 U.S.C. § 107 and applied in federal case law (related to scholarship, research, criticism, and news reporting, for example)—it is also necessary to obtain permission from the copyright holder of the photograph in question. The person or entity creating the photograph is generally the holder of the initial copyright.

The following scenario presents a simple example of the right of publicity. A magazine takes your photograph in connection with a news story about a community event in which you participated and publishes the photograph. You are not entitled to payment, because this use is not connected with trade or advertising. In addition, because the magazine is engaging in news reporting, the activity is absolutely protected by the First Amendment. Artists using your image without your permission may also be protected by the First Amendment.

But let's take our example a step further: Without your knowledge, the photographer puts the photograph portraying your image in a stock photography

database. You have signed no release and granted no permissions. You later find your photograph on a Web site or in a brochure being used to sell tanning lotion. This use has probably violated your right of publicity.

There are two main reasons that federal courts have developed so much of the case law involving rights of publicity. The first is that rights of publicity are usually tied up with other federal questions, such as copyright or trademark law, thus providing a plaintiff with the option to proceed in federal court. For example, if you are already famous, your persona may be considered a trademark. Use of your image might cause consumer confusion, and you may have federal rights under § 43(a) of the Lanham Act for a false endorsement claim.[9] If you are not famous, you may not have access to such federal rights, which may require proving your fame and showing that you have used your name as a trademark.

The second reason that federal courts have created so much case law dealing with the right of publicity is that many of these cases arise under federal diversity jurisdiction, because the cases involve distribution of goods and services via interstate commerce. The choice of law and choice of forum may determine the outcome in such cases; therefore, filing in a district court located in a friendly state may be critical. A recent federal district court decision extinguishing the alleged post-mortem rights of publicity claimed by the heirs of Marilyn Monroe's residuary estate is illustrative.

In 1994, more than three decades after Marilyn Monroe's death, Indiana passed a law granting celebrities descendible and freely transferable post-mortem rights for 100 years after death. In 1984, California passed a law granting post-mortem publicity rights, whereas New York grants no post-mortem publicity rights to celebrities. After Marilyn Monroe died in 1962, her estate went through probate. In 2001, a Delaware company called Marilyn Monroe LLC, was set up to hold the residuary assets of her estate. Marilyn Monroe LLC licensed CMG Worldwide Inc., an Indiana company, to exploit Marilyn Monroe's rights of publicity. In 2005, CMG threatened the Shaw Family Archives with litigation. The Shaw Family Archives owned and licensed the copyright in many iconic Marilyn Monroe photographs, such as the subway grate shot from "The Seven Year Itch." On Sept. 6, 2006, a T-shirt containing Marilyn Monroe's image from this shot and bearing the label "Shaw Family Archives" was allegedly purchased at an Indianapolis Target store. CMG filed suit in Indiana.

Before being served, the Shaw Family Archives filed suit for a declaratory judgment in the Southern District of New York. After motion practice and a decision involving conflicting interpretations of the law, the suit ended up in New York.[10] On May 7, 2007, Judge Colleen McMahon of the Southern District of New York held that the 1994 Indiana law did not apply retroactively to create rights of publicity that Marilyn Monroe did not possess at the time of her death in 1962.[11] Indiana's post-mortem publicity rights law did not grant any rights to the heirs of Marilyn Monroe, because no such rights existed at the time of Marilyn Monroe's death either in Indiana or in New York or California, the places of her domicile and death. The district court's ruling thus shut down a lucrative licensing operation in Indiana.

Elvis Presley's heirs do not share the fate of Marilyn Monroe's heirs. Elvis Presley died at Graceland in Tennessee, and his rights of publicity are governed by Tennessee law. The U.S. Court of Appeals for the Sixth Circuit has affirmed that Elvis Presley Enterprises Inc. owns numerous federal trademarks and Tennessee publicity rights to photographs of Elvis.[12] Tennessee law does not place any express time limits on post-mortem rights of publicity. Thus Elvis's rights of publicity will support a licensing industry for the foreseeable future.

Concerns about rights of publicity are no longer the exclusive province of celebrities. By virtue of the Internet, average Americans have invested in their online identities for commercial purposes and may be entitled to more than their proverbial 15 minutes of fame. The cases of Marilyn Monroe and Elvis Presley illustrate the uncertain role the rights of publicity will play in interstate commerce for years to come. **TFL**

Raymond J. Dowd is a partner with Dunnington Bartholow & Miller LLP in New York City. He is president of the Southern District of New York Chapter of the FBA and a member of the FBA Editorial Board. He is the author of Copyright Litigation Handbook *(West 2007).*

Endnotes

[1]*Herman Miller Inc. v. Palazetti Imports and Exports Inc.*, 270 F.3d 298, 324–326 (6th Cir. 2001).

[2]*Parks v. LaFace Records*, 329 F.3d 437, 460 (6th Cir. 2003).

[3]*Id.* (collecting cases and surveying state statutes).

[4]*Facenda v. NFL Films Inc.*, 488 F. Supp. 2d 491, 501–503 (E.D. Pa. 2007).

[5]*Cuccioli v. Jekyll & Hyde Neue Metropol Bremen Theater Produktion GMBH & Co.*, 150 F. Supp. 2d 566, 575 (S.D.N.Y. 2001).

[6]*Id.* at 324–328.

[7]*King v. PA Consulting Group Inc.*, 485 F.3d 577, 591–592 (10th Cir. 2007) (invasion of privacy claim).

[8]*Flentye v. Kathrein*, 485 F. Supp. 2d 903 (N.D. Ill. 2007).

[9]*Waits v. Frito-Lay Inc.*, 978 F.2d 1093 (9th Cir. 1992).

[10]*Shaw Family Archives Ltd. v. CMG Worldwide Inc.*, 434 F. Supp. 2d 203 (S.D.N.Y. 2006).

[11]*Shaw Family Archives Ltd. v. CMG Worldwide Inc.*, 486 F. Supp. 2d 309 (S.D.N.Y. 2007).

[12]*Elvis Presley Enterprises, Inc. v. Elvisly Yours Inc.*, 936 F.2d 889 (6th Cir. 1991).

MICHAEL NEWMAN AND SHANE CRASE

Family Responsibilities Discrimination

Many attorneys know firsthand the juggling act required of working parents. Employment law practitioners should be keenly aware of the potential legal issues that arise in the workplace when employees request and take family-related leave. The Equal Employment Opportunity Commission (EEOC) recently provided some guidance in order to assist attorneys and employers alike to spot issues that arise in the workplace related to caregivers.

On May 23, 2007, the EEOC issued enforcement guidance on the subject of unlawful disparate treatment of workers with caregiving responsibilities.[1]14 In this guidance, the EEOC highlights the potential for discrimination and harassment of caregivers in the workplace. Who is a caregiver? Caregivers may be mothers or fathers caring for their children, grandparents caring for grandchildren, adult children caring for elderly parents, or family members caring for relatives with disabilities, among others. Although the EEOC emphasized that "caregiver" is not a new protected category, the unique and particular circumstances of caregivers may implicate concerns about discrimination based on gender, pregnancy, race, national origin, and disability as well as the potential claims of creating a hostile work environment and retaliating against employees.[2] For this reason, the EEOC has focused on the application of existing federal laws to caregivers.

The treatment of caregivers in the workplace is of growing importance when trends and statistics are taken into account, such as the following:

- a workforce that consists of more than 46 percent women,[3]
- an increased likelihood that mothers with young children will be employed,14[4]
- the aging of "baby boomers,"
- the potential disproportionate impact of caregiving responsibilities on African-American and Hispanic women,[5] and
- the increased number of men who perform caregiving responsibilities.14[6]

This notion of "family responsibilities" discrimination is not new. In its 2003 decision in *Nevada Department of Human Resources v. Hibbs*, the U.S Supreme Court explicitly found that the Family and Medical Leave Act (FMLA) "aims to protect the right to be free from gender-based discrimination in the workplace."[7] Specifically, the Court examined the language of the FMLA itself, in which Congress expressed that the objective of the legislation is to minimize "the potential for employment discrimination on the basis of sex by ensuring generally that leave is available … *on a gender-neutral basis*. …"[8] The facts of *Hibbs* involved a male employee, employed by the state of Nevada, who used FMLA leave in order to care for his spouse as she recuperated after a car accident and resulting surgery. Examining the remedies provided by the FMLA, the Supreme Court found that the FMLA was designed to provide "a minimum standard of family leave for *all* eligible employees, irrespective of gender," thereby leveling the field for all caregiving employees.

The U.S. appellate courts have examined a variety of cases involving caregivers in the workplace. For example, in *Back v. Hastings on Hudson Union Free School District*, the Second Circuit reversed summary judgment where an elementary school psychologist who had been denied tenure presented evidence of comments that included gender stereotypes.[9] In this case, the employee had been employed by the school district for a three-year probationary period, at the end of which she was to be reviewed for tenure purposes. During this probationary period, the employee had taken maternity leave. Even though the employee had received positive performance evaluations prior to her maternity leave, after she returned from her leave, the employee alleged that her supervisors made several stereotyping remarks about whether the employee could juggle both her career and motherhood. For example, the employee alleged that her supervisor had told her that "maybe [she should] reconsider whether [she] could be a mother and do this job. …" The employee also alleged that her supervisors had expressed concern that once she obtained tenure, she "would not show the same level of commitment [she] had shown because [she] had little ones at home." The employee also alleged that her supervisors had "expressed concerns about [her] child care arrangements, though these had never caused [her] conflict with school assignments." Her supervisors denied that they had questioned or doubted the employee's ability to be both employee and mother; instead, her supervisors alleged that these meetings had been held to discuss the employee's performance. In reversing summary judgment, the Second Circuit found that "*Hibbs* makes pellucidly clear, however, that, at least where stereotypes are considered, the notions that

mothers are insufficiently devoted to work, and that work and motherhood are incompatible, are properly considered to be, themselves, gender-based."[10]

In *Lust v. Sealy Inc.*, the Seventh Circuit affirmed a jury verdict in favor of an employee who sued her employer for sex discrimination.[11] In that case, the employee had clearly voiced her desire to be promoted to a management position. When such a position became available in a city 148 miles away, her supervisor awarded the position to a male. The Seventh Circuit found that the supervisor "admitted that he didn't consider recommending [the employee] for the Chicago position because she had children and he didn't think she'd want to relocate her family, though she hadn't told him that." Addressing this evidence, the court found that "antidiscrimination laws entitled individuals to be evaluated as individuals rather than as members of groups having certain average characteristics." Thus, the *Sealy* court held that the jury's finding that the plaintiff had been denied a promotion because of her gender was not unreasonable.

Similarly, in *Lettieri v. Equant Inc.*, the Fourth Circuit reversed the district court's grant of summary judgment on a female employee's Title VII sex discrimination claim.[12] In that case, the employee alleged that, during an interview for a promotion, a senior vice president of the company had inquired about the employee's weekly commute between New York and Virginia. Specifically, the senior vice president had asked the employee "how [her] husband handled the fact that [she] was away from home so much, not caring for the family" and commented that "he had 'a very difficult time' understanding why any man would allow his wife to live away from home during the work week." The employee was denied the promotion and was ultimately terminated. The court found that a jury could conclude that the employer had demonstrated a discriminatory attitude.

In *Walsh v. National Computer Systems Inc.*, the Eighth Circuit addressed caregiving issues and pregnancy discrimination under Title VII, FMLA, and a state antidiscrimination law.[13] In this case, the employee had taken medical and maternity leave because of complications arising from her pregnancy. Upon returning to work, the employee alleged that she had been subject to increased scrutiny of her hours, including being told by her supervisor that "she must make up 'every minute' that she spent away from the office for doctors appointments for herself or her son and time spent caring for her son," which was not required of other employees. When the employee was absent from work in order to care for her son, her supervisor hung a sign on the employee's cubicle that read "Out—Sick Child," something that had not been done when other employees had been absent. After the employee fainted at work, her supervisor informed her that she had "better not be pregnant again." The employee ultimately brought suit, alleging failure to rehire, hostile work environment, constructive discharge, and retaliation. The jury awarded the employee an amount in excess of $430,000. On appeal, in response to the employee's gender discrimination claim, the employer argued that Title VII does not prohibit discrimination against parents or caregivers. The employee contended that she had been discriminated against on the basis of her "potential to become pregnant in the future." The Eighth Circuit agreed with this legal argument, finding that "potential pregnancy … is a medical condition that is sex-related because only women can become pregnant." Consequently, the Eighth Circuit did not vacate the jury verdict as it related to the employee's claim of gender discrimination.

As these cases illustrate, issues surrounding caregivers in the workplace may arise in a multitude of situations and may implicate a variety of both federal and state laws. As such, both attorneys and employers alike should be mindful of policies and actions in the workplace that may present problems. The EEOC's guidance suggests a number of best practices for employers, including the following:

- considering whether more flexible policies can be implemented in order to accommodate employees' caregiving needs (such as leave or flexible scheduling);[14]
- avoiding asking interviewees and job candidates questions regarding marital status, family planning, or any caregiving responsibilities;
- basing any employment decisions, such as discipline, performance evaluations, or termination, on objective criteria (by doing so, employers can avoid using subjective criteria that may reflect stereotypes surrounding gender and caregiving responsibilities; the EEOC emphasized that even "benevolent stereotyping"—such as denying a promotion and its consequent increased workload so as not to burden an employee with caregiving responsibilities—may be unlawful); and
- providing equal treatment to both male and female caregivers. (According to the EEOC, even though working women have generally borne the brunt of gender-based stereotyping, unlawful assumptions about working fathers and other male caregivers have sometimes led employers to deny male employees opportunities that have been provided to working women or to subject men who are primary caregivers to harassment or other disparate treatment.)

Thus, employers may provide female employees with pregnancy-related leave during periods of incapacity related to childbirth, but employers should take care to identify other reasons for leave, such as for child care, to which both male and female employees are entitled. In conclusion, the EEOC's guidance provides new perspective on protections available to

LABOR *continued on page 49*

JEFFREY C. GOOD

Chief Judge William P. Greene Jr. U.S. Court of Appeals for Veterans Claims

Chief Judge William P. Greene Jr. grew up in Bluefield, a small coal town nestled in a broad valley in the southern Appalachian mountain range of West Virginia. The 1940s was an era of Jim Crow, with almost total segregation between the white and black communities in Bluefield. The only occasions on which he ventured into a white community were when he accompanied his grandparents or parents as they cooked, cleaned, gardened, or performed other domestic chores for white townspeople.

Chief Judge Greene learned the value of hard work from his grandparents, parents, and others in the tight-knit black community. His grandfather, once a schoolteacher, worked on the rail cars that hauled rich bituminous coal from the region's many coal mines. Chief Judge Greene's grandmother worked as domestic help in the home of a white family. His father worked on the railroads while pursuing a degree in music and English from Bluefield State College, an institution originally founded in 1895 as the Bluefield Colored Institute to train African-American teachers for the country's segregated schools. After earning his degree, the judge's father worked as a high school teacher; but on nights and weekends he worked at many other jobs, including jobs at a local newspaper, as a gardener, as a musician, and as a facilities engineer at an elementary school. Chief Judge Greene's mother, also a graduate of Bluefield State College, taught piano and directed the church children's choir.

Chief Judge Greene's father was drafted into the Army shortly after the attack on Pearl Harbor. Like society at the time, the Army was officially segregated; black units required black officers. Because he had a college degree, his father was selected for Officer Candidate School and commissioned as a second lieutenant. Although most African-American units were relegated to support functions, Chief Judge Greene's father was assigned to the 92nd Infantry Division—the famed "Buffalo Soldiers"—the only African-American infantry unit to see combat in Europe during World War II.

After the war, the judge's father rejoined his family in Bluefield. He would have liked to stay active in the Army Reserves, but at the time there were no black units in the active Reserve, and the idea of a black officer commanding white troops was simply unthinkable. Therefore, he was forced into the inactive Reserves. Despite his status as an "inactive" Reserve, Chief Judge Greene's father was one of the first people recalled to active duty during the Korean conflict, where he served for a year, then again returned to his family in Bluefield. Only now, he decided to remain in the Army instead of returning to teaching and his many part-time jobs. He announced that the family would be moving to Fort Knox, Ky.—a daunting prospect for Chief Judge Greene, then nine years old. Other than short jaunts with his grandfather or father on local passenger trains, Chief Judge Greene had barely been outside of Bluefield.

The family arrived at Fort Knox in 1953, shortly after President Truman ordered the armed forces desegregated. His father was assigned an on-post house, and Chief Judge Greene attended one of several elementary schools on the massive Army post. For the first time, Chief Judge Greene had white neighbors and white classmates. He fell into his new routine

quickly and made many lifelong friends.

A few years later, Chief Judge Greene's father was transferred to Oklahoma to head up the ROTC program at Langston University, a historically black college. Chief Judge Greene was again thrust into a totally segregated environment in a small town in Oklahoma, where schools remained firmly segregated even in the wake of the Supreme Court's decision in *Brown v. Board of Education*. Chief Judge Greene attended a laboratory school located on the grounds of the university, where university students honed their teaching skills. Most of the actual teachers had either master's degrees or doctorates. Chief Judge Greene reports that he was "surrounded by an aura of intellectualism and excellence that instilled a lifelong respect for the value of education."

From Oklahoma, Chief Judge Greene's father received orders back to Fort Knox, but a lack of on-post housing required Chief Judge Greene and his mother to return to Bluefield for nearly a year. Chief Judge Greene finished the ninth grade in Bluefield and renewed many old friendships, including one with his future wife, Madeline. The idea of becoming a lawyer began to coalesce in his mind. His experiences in Langston convinced him that he should pursue an advanced degree. He thought about becoming a doctor or an architect, but he struggled with math and chemistry. He received inspiration and encouragement from James Redmond, the only African-American lawyer in the town, where he was widely respected and admired and a leader in the community.

The following year, Chief Judge Greene and his mother rejoined his father at Fort Knox, where the judge became captain of the basketball team and ultimately graduated from the post high school, Fort Knox High. His desire to become a lawyer was widely known among his classmates. In his yearbook, he listed lawyer as his chosen ambition, and the yearbook's cartoonist took the liberty of drawing a caricature of the judge standing at a lectern, apparently making an argument—*in a military uniform*. Although prophetic, at the time Chief Judge Greene had no intention of following his father's footsteps into the Army.

After graduating from high school, Chief Judge Greene attended West Virginia State University, which, according to the judge, "was and is a living laboratory of social change." West Virginia State was one of the first colleges to fully integrate, going from a totally black student body at the time of *Brown v. Board of Education* in 1954 to a 50/50 mix by the time Chief Judge Greene started his studies there in 1961. West Virginia State was a land-grant college, where Army ROTC was a required course. Despite not wanting anything to do with the Army initially, he quickly became gung-ho, polishing his boots with gusto and wearing his uniform with pride. He became the cadet commander and commanded the Pershing Rifles Drill Team. He recounts, "I was sickening, probably." When not engaged with ROTC, he studied political science, because he was still intent on becoming a lawyer one day.

Chief Judge Greene upon retirement from the Army by the Buffalo Soilder Monument at Fort Leavenworth, Kansas.

But his Army ambitions won out temporarily. He accepted an Army commission and was designated to serve with the Armor Branch. He wanted "to jump out of airplanes and be an Army Ranger." Following graduation, he was visiting his father, who was then stationed at Fort Meade near Washington, D.C., while awaiting orders to jump school. His father encouraged him to visit the Army Personnel Command and review his record, advising him to "find out what's going on in your program." Chief Judge Greene got in his car and drove to the Pentagon, not sure just where the Personnel Command was. In a bit of serendipity at which he still marvels, he found himself lost in the byzantine belly of the Pentagon. While wondering around the building's E-Ring, he stumbled across a sign that read "The Judge Advocate General's Corps." While the judge stared at the sign, an officer passed by and introduced himself. Chief Judge Greene asked, "how do you get in JAG, anyway?" The officer brought him into the office and explained the various options—one of which was the "excess leave" program, in which regular Army officers could earn service credit (but not pay) while pursuing a law degree. Chief Judge Greene quickly assembled an application and was accepted, on the condition that he take the LSAT and find a law school that would admit him for the next semester—no mean feat given that it was already June.

He called West Virginia University College of Law but was informed the class was filled. But the former registrar at West Virginia State was now the registrar at Howard University, so the West Virginia registrar sent Chief Judge Greene to him. Luckily, Howard still had an opening and Chief Judge Greene was admitted a scant six weeks before class started. For the next three years, Chief Judge Greene studied at Howard

GREENE *continued on page 18*

GREENE *continued from page 17*

and interned in Army JAG offices at the Pentagon and the military district of Washington, D.C. He also found time to marry his childhood sweetheart, Madeline, and have a son, Billy. Chief Judge Greene graduated from Howard University Law School in 1968, passed the West Virginia Bar, and was commissioned as an officer in the Army Judge Advocate General's Corps.

Chief Judge Greene's first assignment was at his old stomping ground of Fort Knox, where he performed duties as a courts-martial prosecutor and trial defense counsel. At the time, Army courts-martial practice was a high-volume business. In 1968, the Army was the largest it had been since the Korean War, and the majority of the troops were conscripts—many none too happy to be in the Army. When he first arrived in his new office, there were case files stacked several feet high on his desk—cases waiting to be tried. Many of his clients were facing their second or third courts-martial. It was not unusual for him to take four or five clients into court for a mass arraignment and then try their cases one after the other. Chief Judge Greene discovered that he was a natural for trial work. "It was where I belonged," he says. He found that his childhood experiences of learning to get along with a wide variety of people under a wide variety of circumstances gave him a natural rapport with the soldiers. When he wasn't in the courtroom, he spent most of his time in the barracks, talking with his clients, unit leaders, and witnesses. Because military defense counsel have relatively few resources at their disposal, they typically act as their own investigators. He developed a reputation as a fierce advocate, and soon soldiers from all over the post were seeking his services—on cases involving everything from being absent without leave to premeditated murder.

During this time, Chief Judge Greene and Madeline had their second son, Jeff. In 1970, knowing that it was just a matter of time before he received orders to go to Vietnam; Chief Judge Greene decided to take his destiny into his own hands and volunteered. He was told "we'll call you back," and about a month later, he received a return call asking if he'd consider going to Hawaii instead. His first thought was "well, I like this organization." He didn't realize it at the time, but his tour in Hawaii was closely tied to events in Vietnam. Racial polarization and racial tensions in the Vietnamese theater were escalating. Drug use was rampant. Racial confrontations led to violent crimes. There had been a particularly violent race riot at a military prison in Long Bien. The perception, if not the reality, was that a disproportionate number of minority soldiers were being court-martialed. Many black soldiers facing court-martial wanted a black defense counsel, but they hadn't seen any in uniform. At the time, of the 1,500 JAGs in the Army, 12 were African-American and none of them were serving in Vietnam.

Instead of sending an African-American defense counsel into Vietnam—and potentially further exacerbating racial tensions—the decision was made to transfer many of the Vietnam cases to Hawaii for trial. Chief Judge Greene estimates that he tried more than a thousand cases during his three-year tenure in Hawaii. Toward the end of his tour, he received several offers from civilian practitioners to leave the Army and work in private practice in Hawaii. But he had remaining obligated service from the excess leave program, and the Army wouldn't let him resign. Instead, Chief Judge Greene was selected for advanced training at the Army JAG School in Charlottesville, Va.

In 1973, Chief Judge Greene was selected to head up the Army Judge Advocate General Corp's recruiting program. Although he was well-known and well-regarded for his courtroom prowess, this position cemented his reputation as a rising star in the Army JAG Corps. He met or exceeded the Army's JAG recruiting and accession goals, despite the Army's popularity being at an all-time low following the Vietnam War. He increased the number of minority JAGs by 200 percent—from 30 to 90, including the first female African-American JAG officer. Chief Judge Greene proudly points out that he recruited the current leadership of the Army JAG Corps, including Maj. Gen. Scott C. Black, the current judge advocate general of the Army. It was during this tour that Chief Judge Greene began his long association with the Federal Bar Association, where he remains a member of the Pentagon Chapter.

From this post, Chief Judge Greene was off to Wuerzburg, Germany, as the deputy staff judge advocate for the Third Infantry Division, where he put the minor in German language he had earned in college to good use. Among his many other duties, he was called in as an observer under the Status of Forces Agreement when American soldiers were tried in German courts for local offenses.

In 1980, he was selected to attend the Army's Command and General Staff College. He was then assigned as chief of the Criminal Law Division at the Army Judge Advocate General's School in Charlottesville, Va., on the grounds of the University of Virginia. He developed a comparative law class and advanced trial advocacy course attended by JAGs of all the services. Chief Judge Greene also developed a reputation as an expert in military criminal law. By the end of his three-year tour, his oldest son was approaching his senior year in high school, and Chief Judge Greene was facing the prospect of another duty assignment overseas. Instead of uprooting his family for a typical three-year tour of duty, he elected a one-year unaccompanied tour in Korea as staff judge advocate to the Second Infantry Division. Although he missed his family terribly, the conditions were rugged, and the work was relentless, he describes the year as his most rewarding tour of duty. It was here that he felt

he could "put it all together"—drawing on his many varied experiences to be the lead legal adviser dealing with everything from settling minor tort claims to combating black marketing and conducting international diplomacy.

Following his year in Korea, Chief Judge Greene was selected for the prestigious Army War College, a high honor for a JAG, where he studied alongside the future leaders of the U.S. military. Following graduation, he was assigned as the staff judge advocate at the U.S. Military Academy, where he had to face an entirely new set of unique challenges, such as compliance with the rules set by the National Collegiate Athletic Association and academic honor codes. He describes himself as a "West Point groupie" and says he "never wanted leave." He even considered taking a permanent teaching position at the academy.

But the lure of new challenges and new experiences led Chief Judge Greene to accept yet another position as a staff judge advocate—this time at Fort Leavenworth, Kansas, the home of the U.S. military's only maximum security prison. During this tour, Chief Judge Greene was involved in the construction and dedication of the Buffalo Soldier Monument, which was located on the garrison grounds. Chief Judge Greene also began to seriously contemplate his post-Army career. He considered various options, including teaching and politics.

Some years earlier, an old friend of his—the deputy chief U.S. immigration judge at the time—had encouraged Chief Judge Greene to consider taking a position as an immigration judge. Chief Judge Greene submitted his résumé but later decided that he wasn't ready to leave the JAG Corps. Four years later, however, he received another call—this time from a new deputy chief immigration judge, who had come across Chief Judge Greene's old résumé and invited him to interview for a position. Although Chief Judge Greene hadn't yet decided to leave the Army, he thought, "when opportunity knocks, you can't say 'wait, let me pack my bags.'" He flew to Washington for an intense interview and, a short time, later was notified that he had been selected and his name would be submitted to the U.S. attorney general.

But then the reality of leaving the Army hit home. He had been, in effect, a part of the Army since the age of nine. With his stellar record, he was a leading candidate for the highest ranks of the JAG Corps, yet he longed for the opportunity to return to the courtroom, and he knew that, if he wasn't selected for flag rank, he would face mandatory retirement in three years. By then, the opportunity to be an immigration judge might have slipped away. After agonizing over the decision for a few days with Madeline, he came up with an unorthodox, if effective, decision-making method while walking from his on-post house to work one morning. "The left foot is 'yes,' and the right foot is 'no,' and wherever I was when I stopped at my desk, that was going to be the decision." He landed on his left foot and immediately sat down to call Army headquarters to announce his retirement.

Chief Judge Greene with his family.

Three months later, in June 1993, he was appointed as an immigration judge in Baltimore, Md., and also covered Buffalo, Pittsburgh, Harrisburg, and Philadelphia. He found the work of an immigration judge to be grueling, but rewarding. He handled approximately 1,000 cases per year on all manner of immigration matters. He developed a reputation as an exacting, yet compassionate, judge. Throughout it all, he never lost his appreciation for the profound impact his decisions had on the individuals who appeared before him. He notes, in typically understated manner, that "they were important decisions."

Although he was reveling in his return to the courtroom and the work he was doing, opportunity knocked yet again in 1996. Another old friend informed him of a search for potential candidates for appointment as a judge on the U.S. Court of Veterans Appeals. Chief Judge Greene elected to throw his hat in the ring. In early 1997, he was interrupted in court by a phone call from Madeline. Fearing a family emergency, he was relieved and excited to learn that the White House had called and the President intended to nominate him to the veterans' court. After nearly a year of being vetted and confirmed by the Senate, Chief Judge Greene was installed as a judge on the Court of Veterans Appeals on Nov. 24, 1997.

The U.S. Court of Veterans Appeals was renamed the U.S. Court of Appeals for Veterans Claims in 1998. A national court of record, established under Article I of the Constitution, the court has exclusive jurisdiction to provide judicial review of final decisions by the Board of Veterans Appeals (BVA), an entity within the Department of Veterans Affairs. The court itself, however, is completely independent of the department.

Veterans' claims related to entitlement to benefits for service-connected disabilities, educational benefits, vocational training, and other programs are first

GREENE *continued on page 20*

GREENE *continued from page 19*

adjudicated in the various regional offices of the Department of Veterans Affairs; those decisions may be appealed to the BVA. Until 1988, there had been no judicial review of a BVA decision; but in 1988 Congress passed the Veterans' Judicial Review Act, establishing the U.S. Court of Appeals for Veterans Claims, which consists of seven judges, who are appointed to 13- or 15-year terms. The senior judge is designated as chief judge. Chief Judge Greene assumed duties as chief judge on Aug. 8, 2005, when the last of the original seven judges retired.

Chief Judge Greene, as a veteran himself, considers it a great honor to serve on a court that is dedicated to ensuring justice for the men and women who have served our armed forces. He states that he has the "greatest regard for the veterans that come before this court." Life as an appellate judge, however, has taken some adjustment. A gregarious and outgoing man, Chief Judge Greene reports that he misses the almost constant interaction with colleagues, clients, and litigants that he experienced in his former life as an Army JAG and immigration judge. But his experience in high-volume litigation has served him well. The Court of Appeals for Veterans Claims is one of the busiest federal appellate courts in the nation, with the volume of appeals it handles increasing almost daily. At the end of 2005, the court received an average of 200 appeals per month; less than two years later, that number stands at more than 300 per month, with every indication that the increase will continue. Chief Judge Greene describes the sheer volume of cases as the court's most significant challenge, but he says that he looks forward to meeting that challenge with his six colleagues, with whom he greatly enjoys working.

One major project the chief judge hopes to see through in his remaining five years on the court is the construction of a dedicated courthouse in the metropolitan Washington, D.C., area. The court is currently housed in comfortable—albeit nondescript—commercial office space in downtown Washington, D.C. The General Services Administration has completed a feasibility study for construction of a Veterans Courthouse and Justice Center, which will house the court, along with the appellate litigation branches of various veterans service organizations. Chief Judge Greene is hopeful that Congress will support construction of a dedicated courthouse and justice center for veterans as a symbol of gratitude and respect to the veterans and their families who have given so much of themselves in the service of the nation.

In speaking with those who have known and worked with Chief Judge Greene, it is readily apparent that he has an extraordinary talent for building and maintaining personal relationships. Maj. Gen. William K. Suter, USA (Ret.), clerk of the U.S. Supreme Court, has known Chief Judge Greene personally and professionally for more than three decades. Gen. Suter states, "Bill is a wonderful and decent man—no one can say a bad thing about him. He is a bright lawyer, a talented leader, and one with whom you want to associate. He was a splendid Army judge advocate and is respected as a fair and impartial immigration judge and a Court of Veterans Appeals judge." Gen. Suter also notes that Chief Judge Greene is well-known for his keen sense of humor, and smile, "which is always showing." It is also reported that Chief Judge Greene can do a fantastic Ray Charles impersonation.

Chief Judge Greene's personal pursuits include photography, golfing, and traveling to visit with the many friends he and Madeline have acquired over the years. His oldest son, Bill, currently lives in Chicago; his youngest son, Jeff, is an Army physician in San Antonio. Between the two, they have yielded five treasured grandchildren for the chief judge and his wife.

In reflecting upon his career, Chief Judge Greene remarks that he has been extraordinarily lucky. As Thomas Jefferson once commented, "I'm a great believer in luck and I find the harder I work, the more I have of it." And Chief Judge Greene's career is marked by no shortage of hard work. He reports that the words of advice he received from his grandfather upon entering first grade in Bluefield, West Virginia, have served him well—"If a task has once begun. Never leave it till it's done. Be the labor great or small. Do it well or not at all." "Doing it well" aptly characterizes Chief Judge Greene's impressive career of public service. **TFL**

Jeffrey C. Good is the president of the Judge Advocates Association and past president of the FBA Pentagon Chapter. He currently works as an attorney-advisor for the FBI in Washington, D.C.

| *National Election* **Results** |

On Aug. 1, 2007, ballots were counted and verified for FY2008 national officers. Their terms begin Oct. 1, 2007. The president-elect and treasurer will serve a one-year term, which expires on Sept. 30, 2008; directors (group 1–4) will serve three-year terms, which expire Sept. 30, 2010; and vice presidents for the circuits will serve two-year terms, which expire Sept. 30, 2009. Congratulations to these leaders who will serve the association next year.

Board of Directors

President-Elect ..... Juanita Sales Lee

Treasurer ..... Lawrence R. Baca

Group 1 ..... Mark K. Vincent
Qualifier: FBA member in good standing and a current or former FBA vice president of a circuit.

Group 2 ..... Marc W. Taubenfeld
Qualifier: FBA member in good standing and a current or former chair of an FBA section or division.

Group 3 ..... Warren P. Burke
Qualifier: FBA member in good standing and a current or former FBA chapter president.

Group 4 ..... Rene D. Harrod
Qualifier: FBA member in good standing and has served as an FBA chapter officer, a national FBA YLD officer or board member, or as an FBA chapter leader with YLD responsibilities. In addition, at the time of election, the person must be age 36 or younger.

Delegate to the ABA

Delegate ..... Alan C. Harnisch

Vice Presidents for the Circuits

1st Circuit ..... Anthony D. Mirenda

2nd Circuit ..... Glenn M. Cunningham

3rd Circuit ..... James J. West

4th Circuit ..... Stephen R. Jackson

5th Circuit ..... David L. Guerry

6th Circuit ..... David L. Parham

7th Circuit ..... Joel R. Skinner

8th Circuit ..... Anh Le Kremer

9th Circuit ..... W. West Allen

10th Circuit ..... Hon. Robert E. Bacharach

1th Circuit ..... Cynthia M. Van Rassen

D.C. Circuit ..... Brian C. Murphy

Memorials and Remembrances *Gift Program*

With a tax-deductible gift to the Foundation of the Federal Bar Association, members of the legal profession, the public, business organizations, charitable trusts, or other foundations may create a memorial to a deceased person. Gifts may also be made in honor of someone, an anniversary, birthday, or any other occasion. Your gift helps fund educational and charitable programs that promote public understanding of the law and enhance the cause of justice.

Foundation of the Federal Bar Association

Memorial/Remembrance Gift Program

PLEASE DETACH AND MAIL THE COMPLETED FORM TO:
Foundation of the Federal Bar Association
2011 Crystal Drive, Suite 400, Arlington, VA 22202

_____
In Memory of

_____
Date of Death

_____
In Honor of

_____
Occasion

Please send acknowledgment to:

_____
Name

_____
Address

_____
City, State, Zip

Donation made by:

_____
Name

_____
Address

_____
City, State, Zip

NATHAN BROOKS

Safeco Insurance Company of America v. Charles Burr: The Supreme Court and the Business of Consumer Background Information

GRANTED, ANOTHER INSTANCE of the Supreme Court reversing the Ninth Circuit may hardly seem cause for inspection. In its ruling in Safeco v. Burr, however, the Supreme Court did much more than dress down its least favorite appeals court. The case also gave the Roberts Court its first major opportunity to address the Fair Credit Reporting Act (FCRA).

Enacted in 1970, the FCRA represents the federal government's most far-reaching effort to regulate the increasing use of background investigations for a wide variety of corporate purposes. Whereas most people understandably associate the FCRA with credit reporting, the act regulates a much larger group of "consumer reports"—from criminal histories to verifications of social security number—used for pre-employment screenings, loan approvals, and so forth.

To put it simply, the widespread availability of personal information allows businesses to scrutinize potential employees, business partners, and customers more closely. The way in which this information is used has tremendous consequences for the subjects as—for example, a reported criminal conviction can keep a person from gainful employment. For this reason, accuracy and openness are absolutely essential for ensuring the background investigation process is fair to the subject.

Understanding this, Congress (through the FCRA) requires those who use consumer reports to conspicuously disclose to the subject that such reports will be procured and also to alert the subject when the information in a report is the basis for an "adverse action." Under the statute, adverse action in the context of determining insurance premiums is defined as "an increase in any charge for … any insurance, existing or applied for." The notice must also inform the subject how to contact the agency that gathered the information. Armed with this information, Congress reasoned, consumers can better protect themselves against the dangers of inaccurate consumer reports.

The unspoken conflict is that compliance with the law costs businesses time and money; in essence, companies do not want every decision that is based in part on personal information that has been gathered to turn into a time-consuming and expensive mini-trial. For this reason, companies using such information tend to construe requirements narrowly—to the frustration of consumer advocate groups. The question often turns on the existence of an adverse action and, as we will see shortly, the Roberts Court appears willing to allow businesses wide latitude in the formulation of their narrow interpretations.

The questions considered by the Supreme Court in *Safeco v. Burr* involved the insurance industry's use of credit reports, among other things, to determine how much to charge each insurance customer. The justices actually considered two consolidated cases: one involving GEICO and the other involving Safeco Insurance Company.

In the first case, GEICO reported that part of its risk assessment program involved using a variety of information, including credit scores, to place consumers into "tiers" with progressively higher insurance premiums. For the purpose of FCRA's requirements related to adverse actions, GEICO would conduct a "neutralization" analysis, comparing the subject's actual tier placement with that person's placement if the credit score had not been considered at all. Only if this comparison revealed a lower placement on the basis of the credit score would GEICO consider it an adverse action triggering the FCRA's relevant notice requirements.

The Ninth Circuit was not convinced by GEICO's creative interpretation of the FCRA's adverse action requirement. The appeals court pointed out that, by focusing on neutrality as the benchmark for comparison, GEICO failed to consider the possibility that the subject could have received a *more favorable* credit score. This, ruled the Ninth Circuit, is the comparison that the drafters of the FCRA had in mind. In other words, the question is not whether the subject would have paid lower premiums if credit had not been considered; rather, the proper question is whether a lower premium would have been awarded if the subject had a *better* credit score. If the answer is yes, continued the court, then an adverse action has taken place.

In reviewing the facts presented by GEICO, the Su-

preme Court first accepted the insurance company's assertion that, in order for a credit report to be the foundation of an adverse action, it must be a "necessary condition" of the increased premium. Next, the justices moved to the more complicated question of the proper baseline of comparison in determining the occurrence of an adverse action under the FCRA. The Court overruled the Ninth Circuit, reasoning that "Congress was … more likely concerned with the practical question whether the consumer's rate actually suffered when the company took his credit report into account than the theoretical question whether the consumer would have gotten a better rate with perfect credit."

As discussed above, many companies worry about the costs associated with more inclusive definitions of "adverse action." The majority on the Court put great weight on this consideration, noting that an expansive definition not only would make compliance onerous but also would ultimately defeat the purpose of the FCRA: "Since the best rates … presumably go only to a minority of consumers, [an expansive interpretation] would require insurers to send slews of adverse action notices. … We think that the consequences of sending out notices on this scale would undercut the obvious policy behind the notice requirement, for notices as common as these would take on the character of formalities, and formalities tend to be ignored."

The second related case that the Court considered involved the Safeco Insurance Company. As discussed above, the FCRA defines "adverse action" in the context of determining insurance premiums as "an increase in any charge for … any insurance, existing or applied for." Safeco argued that a rate quoted initially could not be an increase and, therefore, could not be an adverse action. In other words, according to Safeco, the use of the word "increase" necessarily required a pre-existing relationship between the customer and the insurance company. The Supreme Court disagreed with this interesting (and ultraliteral) interpretation, finding itself in rare accord with the Ninth Circuit. As the Supreme Court put it, "There is nothing about insurance contracts to suggest that Congress might have meant to differentiate applicants from existing customers when it set the notice requirement; the newly insured who gets charged more owing to an erroneous report is in the same boat with the renewal applicant."

Even though the justices found that Safeco had clearly violated the statute, the company managed to avoid civil liability. The statute only imposes civil liability on a company that "willfully fails to comply" with the law's provisions. In this instance, the Supreme Court equated willfulness with recklessness, reasoning that "a company subject to FCRA does not act in reckless disregard of it unless the action is not only a violation under a reasonable reading of the statute's terms, but shows that the company ran a risk of violating the law substantially greater than the risk associated with a reading that was merely careless."

Using this standard, the Court ruled that Safeco's interpretation was not objectively unreasonable. Not only did the district court agree with Safeco, the justices pointed out, but the company also lacked the benefit of judicial guidance, Federal Trade Commission opinions, or any other official interpretation. Consequently, the Court ruled that "if Safeco did violate the statute, the company was not reckless in falling down in its duty." Put simply, even though the Supreme Court quickly disposed of the company's interpretation of the statute, the justices somewhat confusingly ruled that the company's reading protected it from liability.

In one sense, the Supreme Court's ruling in *Safeco* is limited to a few (albeit significant) groups of businesses, including the insurance industry. The justices did not have the opportunity to address the FCRA's pivotal "adverse action" requirement in other contexts, such as the background investigation for employment purposes. Still, in the broader, more important debate between the business costs of compliance and consumer protection concerns, the justices appear fairly united in their determination to prevent the FCRA from slowing the wheels of commerce. In *Safeco*, the Court (with no dissenting justices) cleared one company of violating the statute and, much more revealingly, shielded from liability another company that had clearly violated the FCRA.

Even though a concurring opinion by Justice Stevens (joined by Justice Ginsburg) criticized the majority for its reasoning as to the GEICO facts, there is very little doubt that, although the decision did not ignore the importance of the protections provided by the Fair Credit Reporting Act, the Court is very concerned about the statute's potential to hurt business. **TFL**

Nathan Brooks serves as general counsel at U.S. ISS Agency, a security consulting firm in Charlotte, N.C., and is a member of the FBA Editorial Board.

Who Should Pay the Price for *Identity Theft?*

The answer to this question appears to be straightforward; obviously, it should be the criminal fraudster responsible for committing the identity theft-related fraud. All too often, however, the fraudsters are not caught; or if they are, there are no funds left to recover. Under current law, financial institutions (FIs) that issue the debit or credit cards often ultimately wind up footing the bill for both fraud related losses and costs of issuing new cards and/or accounts for their customers. FIs are increasingly concerned that data security breaches where hackers or fraudsters steal the "personally identifiable information" necessary to commit identity theft fraud are causing the FIs to suffer more fraud-related losses. The data security breach incident reported by TJX Companies in early 2007 may mark the beginning of a shift in allocation of such fraud-related losses. In addition to consumer class action complaints filed against TJX Companies over the data breach incident, FIs have also filed class action lawsuits targeting retailer and processor liability for data security. FIs have also been involved in lobbying efforts designed to statutorily shift fraud losses and associated costs away from FIs to the entities actually responsible for the data security breach. A legal fight is brewing in both the courts and legislatures over who will ultimately bear the losses of identity theft-related fraud.

By Erin Fonté

Five years ago, if you asked the average person on the street to identify his or her top concerns, only a small percentage would have listed financial fraud resulting from identity theft. Times have changed, however; in a recent study by Zogby Interactive, a vast majority of respondents (91 percent) reported being concerned that their identity might be stolen and used to make unauthorized purchases.[1] Of that 91 percent, 50 percent said they were "very concerned." These survey results are not surprising in light of the proliferation of identity theft and related financial fraud as well as the media coverage of data security breaches that can, and in some cases do, give rise to such identity theft and fraud.

The level of concern about identity theft is understandable, given the dollar amounts at stake. A March 2007 study from Gartner found that from mid-2005 until mid-2006, about 15 million Americans were victims of fraud stemming from identity theft—an increase of more than 50 percent from the estimated 9.9 million victims reported in 2003.[2] The total one-year fraud amount for 2006 is estimated at $55.7 *billion*,[3] and the average number of hours each victim devotes to resolving fraudulent transactions and negative credit reporting issues is thought to be 40 hours per victim.

Consumers harmed by identity theft-based fraud must spend a great deal of time, effort, and money to report and resolve fraudulent transactions, but the financial institutions (FIs) backing the bank accounts, debit cards, and credit cards often bear the brunt of the actual loss attributable to fraudulent transactions. Under federal laws governing FIs and credit card companies, FIs must generally cover most, if not all, losses resulting from identity theft-based financial fraud. FIs that hold the consumer's financial accounts and issue debit cards associated with those accounts or credit cards must generally bear the costs of opening and closing accounts; deposits, transactions, and other payments tainted by the fraud; canceling and reissuing cards (both debit cards and credit cards, as applicable); and refunding fraudulently charged amounts or crediting consumers for unauthorized transactions in accordance with applicable law and rules governing credit cards.

Both state and federal laws generally prohibit identity theft itself as well as the various types of identity theft-based offenses committed via the use of stolen "personally identifiable information" (PII).[4] Victims of identity theft can file police reports regarding their losses. The financial institutions that are affected generally work with law enforcement to help track down and catch the perpetrators, and such institutions can take action as allowed under law to recoup lost funds stolen by fraudsters and other criminals. But all too often, the stolen funds have been transferred to institutions outside of the country or otherwise have been disposed of or converted before the thief is caught. Law enforcement agencies and prosecutors have become increasingly sophisticated in bringing many fraudsters to justice, but identity theft still remains a crime that pays because it can be perpetrated "behind the shadowy cloak of a computer keyboard. … You don't event need to be in the same city or country as your victim. … You can steal someone's identity without being able to speak his language or pronounce her name."[5] Moreover, investigations are increasingly revealing that many identity theft activities are orchestrated and carried out by organized crime rings. In addition, in many instances the crime has two distinct components carried out by two separate and unaffiliated individuals or organizations.

As with any cost, FIs often offset such losses by increasing fees, and FIs may even be able to mitigate some of their losses via insurance coverage. Still, the dollar losses due to identity theft-based fraud represent vast dead-weight economic losses borne by FIs. And with the increase in the number of reports of data security breaches, FIs have begun to notice a common thread among the fraudulent activities. The vast majority of data security breaches involving PII does not originate with FIs but, rather, with government entities, universities and other higher education institutions, retailers (where many day-to-day credit card and debit card transactions occur), and lightly regulated third-party transaction "processors" that aid in routing and processing the credit card and debit card transactions. Fraudsters look for the weakest security in the flow of financial and transactional data so that they can reach into that stream of information to extract the data they want.

On Jan. 17, 2007, TJX Companies (TJX), the parent company of retail chains T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright, announced that an unauthorized intruder had accessed TJX's computer systems that process and store information related to customer transactions for its retail stores, including detailed information about customer debit and credit cards.[6] According to subsequent reports, the number of credit and debit cards that were exposed in this incident reached at least 45 million.[7]

This particular data breach incident could spur a shift in thinking among FIs about identity theft-based fraud. To date, at least 18 separate lawsuits have been filed against TJX stemming from this breach, including two class action suits to hold TJX responsible for the losses the FIs suffered. In addition, legislative efforts are under way in at least seven states that would mandate that negligent retailers pay the costs of the remediation measures that FIs have to take to protect their customers, including dollar losses incurred by FIs because of identity theft-based fraud. Minnesota recently became the first state to enact a law dealing with this issue.

The FIs essentially take the position that unregulated retailers and other entities that do not employ adequate security measures to protect their customers' personally identifiable information should pay the costs of such shoddy security practices. For example, most major retailers have implemented Payment Card Industry Data Security Standards (PCI DSS) to protect credit card data, but only about 19 percent of smaller retailers are in compliance.[8] As a result of fallout from the TJX data security breach, FIs have recently unleashed a series of lawsuits and lobbying efforts aimed at shifting the liability and costs associated with identity theft-based fraud losses to the entities—including retailers—responsible for data security breaches.

This article provides a brief overview of the issues in-

volved in identity-based fraud and the relevant laws apportioning the risk of loss among FIs and credit card associations. In addition, this article will describe the legal fight brewing in both the courts and state legislatures (and potentially the U.S. Congress) over who is to blame for the loss of PII and who should be held responsible for the costs of identity theft-based fraud potentially tied to data security breaches of PII.

What Is Identity Theft, and How Is It Committed?

The ultimate goal of the perpetrators of identity theft is to gain enough information to access a victim's money and/or good credit. Frank Abagnale, a notorious check-fraudster whose story was told in the movie "Catch Me If You Can," became a consultant to financial institutions, law enforcement agencies, and other institutions after he was apprehended and served his sentence. In his book, *Stealing Your Life*, Abagnale made the following observations about identity theft:

> I know cons, and right away I saw that this one was going to be the sweetest of all. For the past 32 years, ever since forsaking my foolish teenage infatuation with perpetrating swindles, I've been a professional expert in how to prevent fraud. … Years before I would never have guessed that [this crime] could even be invented, for it was the most incredible but also the simplest crime ever perpetrated. This festering crime is what we now know as identity theft, the wholesale lifting of someone's identity for illicit gain. It's stealing that identity, then using it to access a person's bank account, their personal information, and their personal finances. It's becoming someone else for the bucks.[9]

Identity theft can start with lost or stolen wallets, pilfered mail, data security breaches, computer viruses, or rifling through paper documents thrown out by individuals or businesses ("dumpster diving"). In addition, as described below, fraudsters use increasingly advanced methods for accessing PII, including "phishing," "pharming," "shoulder-surfing," and "skimming."

Phishing

Phishing allows a fraudster to acquire information—such as user names, passwords, and credit card details—by masquerading as a trustworthy entity in an e-mail or other electronic communication. Frequent targets of phishing attacks have included eBay and PayPal, as well as the Web sites of online banking and financial services. Phishing is typically carried out by e-mail or instant messaging, and often the fraudster's e-mail communication instructs users to type in PII details at a Web site (although telephone calls have also been used in phishing attacks). Phishing also often employs "Web page spoofing," whereby a legitimate Web page, such as an FI's online banking Web site, is reproduced on another server that is under the control of the fraudster, who then captures the customer's PII when he or she attempts to log in.

Many FIs now combat phishing attacks through the use of sophisticated security procedures and anti-phishing programs. FIs have also aggressively educated their customers about ways to distinguish legitimate FI e-mails from fraudulent ones. In recent years, new legislation has made phishing a crime, and more businesses (in addition to FIs) have begun to use customer training and to employ sophisticated anti-phishing software.

Pharming

Pharming is a different type of fraudster attack designed to redirect a Web site's traffic to another site that is a bogus site. Pharming "poisons" a domain name server (DNS) by infusing false information into the DNS, redirecting the user elsewhere even though the user's Web browser displays the intended Web address. Pharming is more difficult to detect than phishing, because all the information from the user's end shows a connection to the legitimate Web site that the user intended to contact. Pharming has become a major concern to businesses hosting e-commerce and online banking Web sites. Protection agains this serious threat requires sophisticated anti-pharming measures; antivirus and spyware removal software cannot necessarily protect against pharming.

Shoulder-surfing

The term "shoulder-surfing" refers to a low-tech fraudster attack using direct observation techniques, such as looking over someone's shoulder, to obtain sensitive PII. Shoulder-surfing is particularly effective in crowded places, such as stores and shopping malls, where fraudsters can simply stand next to someone and watch that person fill out a form and enter a PIN number or a password. Shoulder-surfing can also be done at a distance, with the aid of binoculars or other vision-enhancing devices. In addition, inexpensive miniature closed-circuit television cameras can be concealed in ceilings, walls, or fixtures and data entry can be observed through these devices.

The first line in combating shoulder-surfing attacks, of course, is for individuals to shield their information (PIN number entry activities and the like) from prying eyes. However, new ATMs now employ advanced screen displays that discourage shoulder-surfers; the screen grows darker at a certain angle and the only way to tell what is being entered on the screen is to stand directly in front of it. Certain models of credit card readers have recessed keypads and rubber shields that surround a significant part of the keypad opening. Consumer diligence and these new technological measures can decrease incidences of shoulder-surfing, but this is still one of the easiest ways for a fraudster to get access to PII.

Skimming

Fraudsters can skim the credit or debit card numbers and PINs used in regular retail store transactions by either swapping out a standard point-of-sale (POS) terminal for one that includes a skimming device or modifying a normal POS terminal by attaching a skimming device directly to the terminal. In early 2007, four men were arrested and ar-

raigned on charges of stealing money from the FI accounts of customers of a Stop 'N Shop in Coventry, R.I.[10] Video surveillance showed the four men leaving after allegedly replacing the store's POS terminals with their own terminals. Police investigating this incident believe that the suspects also targeted stores in Cranston, Providence, Bristol, and Warwick, R.I., and may be involved in similar incidents in Las Vegas, Miami, Atlanta, Philadelphia, and Richmond, Va. Law enforcement officials also believe that the suspects may be part of an international organized crime ring. The major advantage fraudsters gain by using skimming techniques is that they can sometimes get information on thousands of cardholders by skimming on only one or two POS terminals.

Where Do Fraudsters Steal Information To Commit Identity Theft?

Fraudsters will generally steal PII from whatever business or entity they can infiltrate to get the information. Numerous colleges and universities have reported data security breaches involving, at a minimum, the names and social security numbers of students and former students. Several FIs have also reported data security breaches ranging from the theft of laptop computers containing unencrypted personal information to unencrypted data tapes falling off document delivery trucks. In recent testimony before the U.S. Judiciary Committee, Joanne McNabb, the chief of the California Office of Privacy Protection, reported the results of her office's survey of 530 data security breaches that have occurred since 2003.[11] Of these incidents, colleges and universities accounted for 28 percent of the breaches; government agencies (federal, state, and local), approximately 24 percent; financial services, 14 percent; medical facilities, 11 percent; retail establishments, 5 percent; and elementary and secondary schools, 5 percent. Manufacturers, data brokers, and other businesses accounted for the remaining 15 percent. Even though there are connections between data security breaches involving PII and the use of PII to commit identity theft, to date there are no conclusive studies about the correlation between data security breaches and whether information from a particular data security breach is actually used to commit identity theft or the rate at which stolen PII is successfully used to commit identity theft.[12]

Who Bears the Costs of Identity-Theft Based Fraud?

Financial Institutions and Electronic Transfers

For many years, the security of PII and financial information was largely the responsibility of FIs (banks, credit unions, savings and loan institutions, and so forth), credit reporting bureaus, and credit card companies. These entities are subject to many rules and regulations regarding privacy and security of PII and requiring FIs to make consumers whole in cases of financial fraud.

The federal Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA),[13] opened up competition among traditional FIs, securities companies, and insurance companies. The GLBA also includes provisions to protect consumers' personal financial information held by FIs. There are three principal parts to the GLBA privacy requirements: the Financial Privacy Rule, the Safeguards Rule, and pretexting provisions.

The Financial Privacy Rule

The Financial Privacy Rule[14] governs the collection and disclosure of customers' personal financial information by FIs. The rule also applies to companies, whether or not they are FIs, that receive such information. FIs must issue and annually update a privacy notice explaining what information is collected about the consumer, with whom such information is shared, how it is used, and how it is protected. The privacy notice must also identify the consumer's right to prohibit sharing his or her PII[15] with unaffiliated parties, as provided for by the Fair Credit Reporting Act.

The Safeguards Rule

The Safeguards Rule[16] requires all FIs to design, implement, and maintain safeguards to protect customer PII. The Safeguards Rule applies not only to FIs that collect PII from their own customers but also to entities—such as credit reporting agencies—that receive customers' PII from other FIs. The Safeguards Rule requires FIs to develop a written information security plan detailing what procedures and mechanisms the FI employs to protect customers' PII on an ongoing basis. The Safeguards Rule also applies to any PII of former customers of the FI that the institution maintains. An FI's data security plan must include the following steps:

- designating at least one employee to manage the data protection safeguards;
- constructing a thorough risk management profile for each department within the FI handling the PII;
- developing, monitoring, and testing a program to secure the PII; and
- changing the data protection and safeguards as needed with the changes in how PII is collected, stored, and used.

The Safeguards Rule generally forces FIs to take a closer look at how they manage PII and to perform a risk analysis on their current processes.

Pretexting

The pretexting provisions of the GLBA protect consumers from individuals and companies that obtain their PII under false pretenses, a practice known as pretexting.[17] Pretexting (sometimes referred to as "social engineering") occurs when someone tries to gain access to PII without proper authority to do so, often by impersonating the account holder by phone, mail, or e-mail. The GLBA has provisions that require the FI to take all precautions necessary to protect and defend the consumer's PII from all varieties of pretexting efforts.

In addition to the GLBA's provisions, FIs are also subject to the federal Electronic Funds Transfer Act (EFTA), which generally governs electronic transfers, including

debit card and ATM transactions.[18] In implementing the EFTA, the Federal Reserve Board promulgated Regulation E, which lists the rights, liabilities, and responsibilities of participants in electronic fund transfer (EFT) systems, such as ATM transfers, telephone bill-payment services, POS terminal transfers, and preauthorized transfers from or to a consumer's account (such as direct deposits and social security payments).

Regulation E imposes limitations on the financial liability of consumers for an unauthorized EFT resulting from loss or theft of an EFT "access device." If the consumer's "access device and secret code" (that is, card and PIN number) are lost or stolen and the consumer notifies the FI prior to any unauthorized transfers, the consumer may avoid monetary loss. After receiving the report of the loss or theft, the FI typically switches off the access device and issues a new one or may even close the consumer's old account and open a new one.

If, in the same situation, the perpetrator makes an unauthorized EFT but the consumer notifies the FI within two business days of discovering the EFT, then the consumer's loss is generally limited to the amount of the unauthorized EFT, up to a maximum of $50. If the consumer waits more than two business days after learning of the unauthorized EFT to report it, however, then the consumer may be liable for losses up to a maximum of $50 for the losses suffered within the first two business days, *plus* an additional $500 if the FI can establish that the loss would not have occurred if the consumer had notified the FI within the first two business days. In addition, a consumer can also lose this $500 liability limitation if he or she waits more than 60 days from the date on which the account statement showing the unauthorized EFT is mailed or otherwise transmitted to the consumer. However, given the way the Regulation E provisions work, most individuals who suffer unauthorized EFTs related to debit cards and/or ATM cards generally lose no more than $50 if they notify their FI.

Credit Card Associations and Credit Card Transactions

The use of credit cards is governed by a different set of laws but, in general, these laws also provide for consumer protection in the event of fraudulent purchases. Under the provisions of the Fair Credit Billing Act,[19] consumers generally have zero liability for fraudulent purchases when they can provide evidence of fraud. The credit card associations operate via a collection of contracts between the FI issuing the credit cards (the issuing FIs), any third-party processors responsible for processing credit card transactions, and merchants that accept the credit cards for payment. Generally, the operating rules of the credit card associations require the issuing FIs to implement the "zero liability" policy for fraudulent credit card charges, and thus the issuing FIs ultimately must absorb the costs of such fraudulent charges.

The credit card associations have also implemented data security standards for merchants and transaction processors that are part of the respective card networks. The newest version of these security standards, mentioned above, is the PCI DSS. The PCI DSS were created by five major credit card companies—Visa International, MasterCard Worldwide, American Express Co., Discover Financial Services LLC, and Tokyo-based JCB Co.—to protect credit card data before, during, and after transactions.[20] Merchants were required to implement the new PCI DSS standards by 2005, but the percentage of small merchants that are PCI DSS-compliant remains low—about 18 percent. The PCI DSS (similar to the Cardholder Information Security Program) generally prohibits merchants from "retaining and storing magnetic-stripe data" from a card after the POS transaction has been completed.

Current Allocation of Financial Liability for Fraud

The allocation of financial liability for identity theft-based fraud falls heavily on FIs. Even though the FIs can generally raise certain fees charged to customers or merchants, the FIs still bear a great deal of the costs of the fraudulent transactions, along with attendant costs of responding to data security breaches (such as closing and re-opening potentially compromised accounts or issuing new debit/ATM and credit cards). The FIs on the back end of processing and settling electronic funds and credit card transactions are subject to extensive examinations and rules, including strict privacy and security requirements. However, retailers and merchants on the front end of electronic funds transfers and credit card transactions, as well as other government and educational entities and businesses that store PII, are lightly regulated or unregulated and, in the view of many FIs, are falling down on the security front and creating security weaknesses in the financial transaction data stream.

Despite protestations from many businesses (especially small businesses) that the costs of increased security requirements could place enormous financial burdens on them, FIs are responding to the TJX security breach with an "enough is enough" attitude. For the first time a concerted industry effort is now under way to shift at least some liability from FIs to those parties arguably responsible for the breaches. This effort is occurring on both the judicial and legislative fronts.

Overview of Court Cases Regarding Data Security Breach Liability

The case law governing data security breaches is understandably sparse, given that reports of such breaches date only to 2003. In one recent Minnesota case, however, the plaintiff lost a tort claim for damages against a financial loan services company that suffered a data security breach.[21] In that case, the Brazos Higher Education Service Corporation, a provider of student loans, faced a lawsuit after an employee's laptop computer, which contained unencrypted PII for roughly 550,000 customers of the company, was stolen from his home. Although none of the information was reportedly used to defraud any Brazos customer, one customer, Stacy Guin, sued Brazos for negligence, alleging the following:

- Brazos owed Guin a duty to "secure private personal

information and not put it in peril of loss, theft or tampering";
- Brazos breached the duty; and
- Guin was damaged as a result.

Guin claimed that, because Brazos is a financial institution, the GLBA requires the company to ensure the "security and confidentiality of customer records and information" from foreseeable and anticipated threats.

Guin argued that Brazos breached the statutory duty imposed by the GLBA. The court determined, however, that Brazos had adequate written security policies and risk assessment reports in place and used sufficient safeguards to prevent acquisition of its customers' information. Moreover, the court found that Brazos was in compliance with the GLBA, which neither requires specific safeguards nor mandates that all personal information be encrypted, according to the court. Rather, the court ruled, the statute merely requires "reasonable measures to protect [personal] data" from foreseeable risks and, in the court's opinion, Brazos had implemented such measures.

Guin argued that the theft of the laptop computer was reasonably foreseeable, because allowing PII to remain unencrypted on an unsecured computer increases the risk of theft. In addition, Guin noted that this particular theft was foreseeable because of the company's knowledge of similar thefts in the financial industry. The court concluded, however, that the Brazos employee himself was not aware of any previous burglaries in his block or in his immediate neighborhood, and therefore "[t]here is no indication that [the Brazos employee] or Brazos could have possibly foreseen the burglary which took place on September 24, 2004."[22] The court also pointed out that there was no evidence that a third party had gained access to any PII. It is unclear whether courts analyzing a similar negligence claim in the future would issue a ruling similar to the one rendered in the *Guin* case, particularly given changing industry practices and standards regarding encryption of PII.

In another case focusing on transaction processing requirements, the plaintiff, Sovereign Bank, incurred losses when its customers' credit card numbers and associated account information were stolen from the computer databases of BJ's Wholesale Club.[23] The security breach occurred between July 2003 and February 2004, and after discovery, Visa notified all individuals whose PII and card information was potentially compromised. Sovereign Bank brought claims against BJ's Wholesale Club and its transaction processor, Fifth Third Bank.[24] As previously discussed, Visa has implemented operating regulations that govern all members participating in the Visa system (FIs that issue credit cards, third parties or FIs that serve as card transaction processors, and merchants who accept Visa cards) as well as information security requirements to protect cardholders' data. Both the Visa operating regulations and the card data security requirements prohibit merchants from retaining and storing magnetic-stripe data from a credit card after the POS transaction has been completed. Sovereign Bank alleged that Fifth Third consistently retained and stored the magnetic-stripe data after transactions were completed in violation of the operating rules and card data security requirements.

Sovereign claimed that, because Fifth Third had violated the contract with Visa (via the operating rules), Sovereign could recover damages against Fifth Third as a third-party beneficiary to the Visa contract. The court determined, however, that Sovereign was merely an incidental beneficiary of the contract and would receive a benefit from the prohibition on the retention of magnetic-stripe data, but that alone was insufficient to make Sovereign an intended beneficiary. Instead, the court found that the operating instructions were intended to benefit the Visa system as a whole and not the specific entities (such as Sovereign) participating in the system. Therefore, Sovereign could not step into Visa's shoes to enforce the operating regulations.

These two cases are important, because they highlight many of the claims and issues alleged in the numerous other cases (approximately 18) currently filed against TJX. In *Mace v. TJX Companies Inc.* (filed Jan. 29, 2007), the plaintiff, Paula Mace, claimed that she had shopped at T.J. Maxx in December 2006 and was notified in January 2007 that her financial information had been compromised because of the corporation's data security breach incident.[25] The plaintiff class consists of other consumers, like Mace, whose personal and financial data had been exposed by the breach. The claim is based on a theory of common law negligence; according to Mace, TJX owed a duty to exercise reasonable care to safeguard all PII in TJX's possession. In addition, Mace alleges that the PII was "improperly stored and inadequately safeguarded in violation of … industry rules and regulations." Under this theory, using credit card industry standards and regulations as the standard of care, TJX breached its duty by failing to comply. The plaintiffs also argue that TJX had a special fiduciary duty to the class members (who entrusted TJX with valuable PII), that TJX had a duty to protect the plaintiffs' right to privacy, and that TJX had a duty to disclose the breach in a timely manner.

Mace claims that TJX breached all these duties, and the class members suffered damages—including fraudulent charges, loss of financial and personal information, and so forth—as a proximate result of the breach. Although it is unclear how the court will rule in this case, the central issue is likely to be the extent of the duty TJX owed to its customers. Is TJX subject to GLBA? If so, did TJX have adequate security procedures in place? Another central question will be whether the breach and its consequences were foreseeable.

TJX also faces suit from a group of FIs in *AmeriFirst Bank v. TJX Companies Inc.* (filed Jan. 29, 2007). According to reports of the TJX breach, many banks and FIs have reported stolen credit cards and fraudulent charges stemming from the TJX breach incident, with fraudulent activity occurring in Florida, Georgia, and Louisiana as well as overseas.[26] The breach exposed credit card and debit card information, driver's license data, and checking account information "linked to transactions for returned merchandise."[27]

AmeriFirst Bank brought a class action suit on behalf of itself and similarly situated FIs against both TJX and Fifth

Third Bank (the third-party transaction processor for TJX). The plaintiffs filed claims of negligence, breach of contract, and negligence per se. First, the plaintiffs claim that the defendants were negligent in that they breached the duty of care and unreasonably delayed reporting the security breach to consumers. Second, as in the *Sovereign* case, the plaintiffs' claim that they are third-party beneficiaries of the agreements between the defendants and credit card associations and can therefore enforce the agreement against the defendants. Third, the plaintiffs allege that the defendants are covered entities under the GLBA, and the defendants' failure to comply with the statute's requirements or industry standards constitutes negligence per se.

When evaluating the contract claim, the court may look to the Pennsylvania case involving BJ's Wholesale Club as persuasive authority that AmeriFirst and other banks are not intended third-party beneficiaries of the contracts between merchants and credit card associations. The third claim, however, raises the critical and novel issue of whether Fifth Third and TJX are "financial institutions" covered by the GLBA with respect to Fifth Third's activities in processing transactions and TJX's role as a retailer initiating such transactions.

The GLBA defines a "financial institution" as any institution that engages in financial activities described in 12 U.S.C. § 1843(k). This provision also brings within the statute's ambit several classes of activities that are financial in nature[28] under Regulation Y, which provides an extensive list of such nonbanking activities. Regulation Y classifies data processing and data transmission services (as long as the data are financial, banking, or economic in nature) as "financial" in nature, which would seem to include Fifth Third, the processor for TJX's credit and debit card transactions.

In contrast to Fifth Third, TJX is the parent company of a large conglomerate of retail stores and arguably does not engage in any activities covered by the GLBA. TJX's operations as a retailer may not be considered financial in nature under the categories listed in U.S.C. § 1843(k)(4) or Regulation Y. Furthermore, according to *American Bar Association v. Federal Trade Commission*,[29] Regulation Y was promulgated to identify nonbanking activities so closely associated with financial activities that they "may be engaged in by a bank holding company or its subsidiary in accordance with the requirements of [the] regulation." Therefore, the court may ultimately decide that, because the business activities of TJX (operating retail chains) are not closely related to traditional banking activities, TJX is not a covered financial institution under the GLBA.

The Massachusetts Bankers Association (MBA) filed a separate class action suit against TJX on April 25, 2007,[30] outlining five claims: (1) negligent misrepresentation, (2) unlawful and deceptive acts and practices in violation of Massachusetts law, (3) violation of the GLBA and unlawful and deceptive acts and practices in violation Massachusetts law, (4) negligence, and (5) breach of contract. MBA first claims that TJX, by participating in the Visa and MasterCard systems, represented that it would comply with the applicable operating regulations imposed by the credit card associations on any entity participating in the systems. In addition, MBA maintains that TJX knew or should have known that it was not in compliance with the rules—specifically the rules prohibiting retention, storage, or disclosure of the magnetic-stripe information obtained from customers' credit and debit cards. The class member FIs, the complaint reads, justifiably relied on the representation that TJX was in compliance with the card association operating regulations, including card data security requirements, and suffered damages as a result. Second, according to the complaint, TJX misrepresented its compliance with the operating regulations and failed to safeguard customers' data, constituting deceptive acts and unfair trade practices under Massachusetts law (TJX is headquartered in Massachusetts).

Third, MBA alleges that the GLBA imposes a duty on TJX "not to misuse or inappropriately disclose information" of customers. By storing the magnetic-stripe information, TJX "maintain[ed] the data well beyond the permitted timeframe" and "allow[ed] the data to be accessed by others for purposes unrelated to the processing of the credit or debit transaction." Finally, the complaint argues that the breach of the GLBA is also a violation of Massachusetts' unfair and deceptive trade practices statute (a claim that similar to the claim raised in the *AmeriFirst* case discussed above).

The final two claims assert negligence and breach of contract theories. The negligence claim alleges that TJX had a duty to provide "adequate" security to customers, and TJX breached this duty by allowing an unlawful intrusion into its system. Finally, similar to the *Sovereign* and *AmeriFirst* claims, MBA claims to be a third-party beneficiary of the agreement between TJX and the credit card operators.

The claims pending against TJX—especially those filed by the FIs—may have a significant impact on the allocation of liability for data security breaches and associated identity theft-based fraud. However, many FIs are not waiting for the outcome of these and similar cases. Instead, they are pursuing lobbying efforts to shift the allocation of liability via statute.

Overview of Legislative Attempts to Shift the Financial Liability for Data Security Breaches and Related Fraud

In seven state legislatures, bills were introduced in 2007 to shift the allocation of liability and costs associated with data security breaches. As of the writing of this article, three of those bills have died, three are still pending, and one was enacted. Minnesota became the first state in the United States to enact legislation that would shift costs and liabilities from FIs to the entities responsible for the data security breaches.

California

California Assembly Bill 779 is the mildest of the legislative measures in terms of the costs and liabilities the bill would shift away from FIs. The bill would clarify that retailers are subject to California data security breach notice requirements (although those entities are arguably already

covered under current law) and would prohibit covered persons or entities from maintaining, storing, retaining, or failing to limit access to customer data after a transaction (which would essentially codify a good portion of the PCI DSS requirements in the California statute).[31]

In contrast to the broader expense reimbursement provisions of legislation proposed this year in Connecticut, Illinois, Massachusetts, Minnesota, New Jersey, and Texas, the California bill's reimbursement requirements would apply only to the cost of the notice itself in situations where a third party company that maintains (rather than owns) data suffers a data security breach (for example, when a data storage facility that stores PII for another business is hacked). In such a case, the actual owner of the information must bear the cost of giving notice under current California law. However, under the California bill that was introduced in 2007 and is still pending, if notice of a data security breach is required, the owner or licensee of the information would be entitled to reimbursement from the third-party entity maintaining the computerized information for "reasonable and actual costs of providing notice to consumers regarding the breach," if the third party-entity that merely holds or maintains the PII suffered or was otherwise responsible for the data security breach. The "reasonable costs" would also include the costs of replacing debit or credit cards in relation to the breach.

Connecticut

Connecticut Senate Bill 1089 would have imposed notice and liability requirements on any person doing business in Connecticut who "owns, licenses or maintains computerized data that includes personal information."[32] The bill's notice provisions would have required that, in the event of a data security breach, all state residents whose personal information may be compromised must be given adequate notice in a reasonably prompt manner. The proposed bill would have imposed liability on any covered person to an FI with customers whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through a breach of security. Liability would include costs incurred by FIs, including the following:

- cancellation or re-issuance of any credit card, debit card or other "account access device";
- closure of any deposit, transaction, or other account as well as other actions to stop payment or block transactions on such an account;
- opening or reopening of any account;
- any refund or credit given to any customer resulting from an unauthorized transaction; and
- any assistance provided to customers to help mitigate loss or inconvenience or to prevent further loss or inconvenience.

Although this measure did not pass, the Connecticut bill would have shifted a significant amount of economic liability from FIs to entities responsible for a data security breach.

Illinois

The state's Credit Card and Debit Card Liability Act,[33] S. 1675, which is currently pending, would amend Illinois law to impose liability on data collectors in the event of a data security breach. The bill would impose liability on the data collector when—

- a credit card or debit card is used to purchase something of value;
- the purchase is made without the consent or authorization of the card's owner; and
- the unauthorized purchase is made as a result of a security breach of the system operated by the data collector, including any breach by an employee or agent of a data collector.

The proposed law would hold the data collector liable to any FI that incurs costs in connection with the unauthorized access to accounts, cards, or funds, including the same costs generally listed under the bill proposed in Connecticut.

Massachusetts

Massachusetts H.R. 213 would impose procedures on "commercial entities" that maintain PII. The bill would add a new chapter entitled "Personal Data Protection," that would have defined the "commercial entities" responsible for providing notice to consumers and/or FIs in the event of a data security breach and would enact liability provisions for those individuals and entities required to give notice under the chapter. The bill would also include additional liability provisions for data security breaches. Any commercial entity required to provide notice to a consumer or an FI would also be liable to any FI for the same costs generally listed under the Connecticut bill. The merchant breach liability provision was not specifically incorporated into a separate omnibus data security bill; therefore it is not likely that the bill will be passed during this session in Massachusetts (although the separate data security breach notice provisions are likely be enacted).

Minnesota

It is important to note that, whereas approximately 38 states have enacted laws mandating notice to consumers of data security breaches, Minnesota recently became the first state to legislatively shift costs associated with data security breaches to the entity responsible for the breach. House File 1758 provides that a person or entity doing business in Minnesota that accepts a credit, debit, or stored value card must not retain or store "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data" after a transaction has been authorized or, for a PIN debit transaction, beyond 48 hours after the transaction. In addition, the bill requires any person or entity responsible for the breach (or such person's or entity's service provider) to reimburse the FI that issued any affected card for reasonable costs incurred to remedy

the breach (generally, the same costs as those detailed in the Connecticut bill). In addition to reimbursement of costs, the bill gives an FI injured by a violation of the bill's provisions a private right of action against the person or entity responsible for the violation.[34]

New Jersey

The New Jersey measure, A. 4413, would prohibit the state's retailers from retaining transaction authorization data (other than name, account number, and expiration date) from a debit or credit card for longer than the amount of time needed to process the transaction. In addition, the measure would make businesses and government agencies that give notice of a data security breach under New Jersey law liable for resulting costs incurred by FIs (generally, the same costs as those listed in the Connecticut bill). The New Jersey bill is still pending.

Texas

House Bill 3222 would have provided that a business that collects, stores, or maintains "sensitive personal information" must abide by generally all the PCI DSS requirements.[35] In addition, an FI would have been given a statutory right to, under certain circumstances, bring claims against a business involved in a data security breach if that business did not comply with PCI DSS requirements at the time of the breach. Under the bill, the FI would have been able to recover all costs generally listed under the Connecticut bill discussed above. The Texas legislature failed to enact H.B. 3222 before the end of the legislative session.

Conclusion

The outcome of the various cases filed regarding the TJX security breach is uncertain. It is also not clear if other states will follow Minnesota's lead in statutorily shifting liability and costs of identity theft to the entities responsible for data breaches. There has been some discussion of a federal data security breach notice law, and Rep. Barney Frank (D-Mass.), chairman of the House Financial Services Committee, has commented that there could be some provisions designed to shift liability from financial institutions to retailers.

One thing is for certain: With the increase in losses suffered by FIs resulting from data security breaches and identity theft-based fraud, FIs are attempting to shift those costs to retailers the FIs believe to be the "weak link" in the security of PII and data related to financial transactions. Retailers claim that these costs will be too high for them to bear, and FIs already pass the costs of such losses along to retailers in the form of interchange fees for processing debit and credit card transactions. Caught up in this struggle are credit card associations, which are under pressure to increase fines against retailers to improve PCI DSS compliance but also need retailers to participate in their networks.

These issues set the stage for numerous court battles and legislative lobbying efforts by FIs, credit card associations, and retailers. The next several years, then, could see a dramatic shift in thinking about who bears the losses associated with electronic financial transactions and what level of data security protection should be required. **TFL**

Erin Fonté is an associate with Los Angeles office of Pillsbury Winthrop Shaw Pittman LLP. Her practice includes a variety of corporate matters. She focuses on counseling financial services clients on a variety of issues, including technology issues, rights to financial privacy, protection of customer data, and compliance with data security regulations. She can be reached at erin.fonte@pillsburylaw.com. *The author wishes to thank Seth Eaton, a third-year law student at Pepperdine University School at Law, for his research assistance on this article.*

Endnotes

[1]*Most Americans Worry About Identity Theft, According to Poll*, GOVERNMENT TECHNOLOGY, April 5, 2007, available at www.govtech.net.

[2]It should be noted that the 2003 statistics came from a Federal Trade Commission study, and the 2006 statistics came from Gartner's own study, hence there are different statistical methodologies.

[3]Privacy Rights Clearinghouse, *Summary of Recent Surveys and Studies from Javelin Strategy & Research, Better Business Bureau, Identity Theft Resource Center, Federal Trade Commission, Gartner, and Privacy & American Business*, last updated June 2007, available at www.privacyrights.org/ar/idtheftsurveys.htm.

[4]This article refers to the theft or security breach of an individual's "personal financial information," but the reader should be aware that definitions of what type of information gives rise to privacy rights and data security breach rights and responsibilities varies under federal and state laws. Use of PII in this article generally refers to a person's name, mailing address, telephone number, bank/FI account information, or other information that may allow a fraudster to commit identity theft.

[5]Frank W. Abagnale, STEALING YOUR LIFE at 4 (Broadway Books, 2007).

[6]Complaint at 3, *Mace v. TJX Cos. Inc.*, No. 1:07 Civ. 10162 (D. Mass. filed Jan. 29, 2007).

[7]CNN Money, *Lawsuits Mount Over Massive Data Breach at TJX Cos*, June 7, 2007, available at money.cnn.com/news.

[8]CRM Buyer, *Retailers Failing to Meet Customer Data Security Standard*, June 13, 2007, available at crmbuyer.com.

[9]*See* n. 5 *supra* at 3–4.

[10]Associated Content, March 3, 2007, available at www.associatedcontent.com.

[11]Joanne McNabb, Chief, California Office of Privacy Protection, "Identity Theft: Innovative Solutions for an Evolving Problem," Testimony Before the U.S. Senate, Committee on the Judiciary, March 21, 2007, available at judiciary.senate.gov.

[12]On July 5, 2007, the Government Accountability Office released a study that concluded that, of the 24 largest data breaches reported between December 1999 and June 2005, stolen information was used in only four instances to create new accounts or to make fraudulent purchases. How-

ever, the report concludes that the full extent of identity theft from large-scale data breaches is unknown. *See* BNA: Privacy Law Watch, *GAO Says ID Theft-Data Breach Link Limited; Backs Risk Threshold for Federal Notice Law*, July 6, 2007, available at pubs.bna.com.

[13]Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

[14]The Financial Privacy Rule is codified at 15 U.S.C. § 6801 through § 6809.

[15]The GLBA uses separate terminology, "non-public personal information," but for analysis under this article, this term is essentially the same as PII.

[16]The Safeguards Rule is also codified at 15 U.S.C. § 6801 through § 6809.

[17]Pretexting provisions are codified at 15 U.S.C. § 6821 through § 6827.

[18]The Electronic Funds Transfer Act is codified at 15 U.S.C. 1601 *et seq*.

[19]The Fair Credit Billing Act is codified at 15 U.S.C. 1601 *et seq*.

[20]Marc L. Songhi, *Retailers Fume Over PCI Security Rules*, COMPUTERWORLD, June 7, 2007, available at computerworld.com.

[21]*Guin v. Brazos Higher Educ. Serv.*, 2006 WL 288483, at 1–2 (D. Minn. 2006).

[22]*Id*. at 13.

[23]BNA: Privacy Law Watch, *Data Security: Contract Claim Against Card Processor Dismissed in BJ's Club Data Breach Case*, June 28, 2006, available at pubs.bna.com.

[24]*Sovereign Bank v. BJ's Wholesale Club Inc.*, No. 1: CV-05-1150 (C.D. Pa. filed June 16, 2006), at 5–6.

[25]*Mace v. TJX Companies Inc*.

[26]Donald G. Aplin, *Data Breaches: Class Claim Alleges TJX Negligently Failed to Adhere to Credit Card Security Standard*, BNA: Privacy Law Watch, Jan. 21, 2007, available at pubs.bna.com.

[27]Complaint at 2, *AmeriFirst Bank v. TJX Companies Inc.*, No. 1:07 Civ. 10169-JLT (D. Mass. filed Jan. 29, 2007).

[28]According to Regulation Y, the following activities are declared to be financial in nature:

> (A) Lending, exchanging, transferring, investing for others, or safeguarding money or securities.
>
> (B) Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death. …
>
> (C) Providing financial, investment, or economic advisory services. …
>
> (D) Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.
>
> (E) Underwriting, dealing in, or making a market in securities.
>
> (F) Engaging in any activity that the Board has determined, by order or regulation that is in effect on November 12, 1999, to be so closely related to banking or managing or controlling banks as to be proper incident thereto. … 12 U.S.C. § 1843(k)(4).

[29]*Am. Bar Ass'n v. Fed. Trade Comm'n*, 430 F.3d 457 (D.C. Cir. 2005), holding that the regular activities of lawyers and law firms do not fall within the definition of "financial services" under the GLBA.

[30]Complaint at 2, *Massachusetts Bankers Ass'n v. TJX Cos. Inc.*, No. 1:07 Civ. 10162-WGY (D. Mass. filed April 25, 2007).

[31]A.B. 779, 2007–2008, Reg. Sess. (Cal. 2007) (as amended May 14, 2007).

[32]S.B. 1089, Gen. Assem., Jan. Sess., § 1(b) (Conn. 2007).

[33]S.B. 1675, 95th Gen. Assem., Reg. Sess., § 3.01 (Ill. 2007).

[34]H.F. 1758, 85th Leg., Reg. Sess., (Minn. 2007).

[35]H.B. 3222, 80th Leg., Reg. Sess., § 1 (Tex. 2007).

Internet Protocol Version 6: *Data Security and Privacy Concerns with the New Internet*

By Michael W. Hubbard

The implementation of IPv6 is important to the technological competitiveness of Europe. However whilst the rapid deployment of IPv6 should be encouraged, this should not be at the expense of safeguarding certain important principles.

> —*IPv6: Legal Aspects of the New Internet Protocol* (Euro6IX 2005)

All organizations will need to develop security plans and policies for dealing with IPv6 traffic, regardless of their decisions whether and when to transition to IPv6.

These realities, coupled with the fact that bad actors are rapidly adopting IPv6 and are already using it to initiate attacks and hide malicious processes and communications, suggest that all organizations should develop explicit plans to provide, or prevent, IPv6 communications. Failure to do so will create the real potential that IPv6 will appear and be used on an organization network either by accident or for malicious intent.

> —U.S. Department of Commerce, National Institute of Standards and Technology, National Telecommunications and Information Administration, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (January 2006)

Suppose that a manufacturer could instantly locate and track every item in stock in real time, whether the item was on a shelf in Beijing or a truck in Boston. Or imagine that, within seconds of a crash on the interstate, police and rescue crews already had critical information about the wreck and the vehicles involved. Or imagine that monitoring sensors on a bridge can communicate in real time with a bridge safety officer.

Such advances are right around the technological corner, thanks to Internet Protocol Version 6 (IPv6), the new language that allows devices to communicate via the Internet. IPv6 technology will allow for a more powerful, more flexible, and more portable Internet, from which businesses stand to reap great benefits.

But user privacy and data protection remain key concerns with respect to IPv6, just as they are with the current protocol version, IPv4. Protecting the privacy of Internet users is essential to the success of IPv6. Commentators on both sides of the Atlantic have raised concerns about privacy as it relates to implementation of the latest protocol.

IPv6 provides a near-limitless number of Web addresses. The change from 32-bit IP addresses to 128-bit IP addresses will allow the Internet—and internal networks—to be used in ways not currently possible.

One of the primary benefits of the Internet—the ability to transmit huge amounts of data around the world instantaneously—is also its major weakness when it comes to data protection. Vast amounts of information about Internet users are collected each day—sometimes without their knowledge or consent. As people conduct more and more of their business online, they are leaving a larger electronic footprint for would-be thieves to follow and ultimately raid. Viruses, Internet worms, spam, botnets, spoofing, and other forms of online attacks have so far proven a difficult problem to contain, and a conversion to IPv6 will introduce new challenges to ensuring user privacy and data security.

What Is IPv6 and How Will It Affect Businesses?

IPv6 is the latest edition of the platform that supports the entire Internet. The current version, IPv4 (IPv5 never got off the ground), has existed for 20 years and is considered by many to lack the capacity that businesses will demand in the future. Experts have been calling for a next-generation Internet Protocol since 1991.

That update is now here. All U.S. federal agencies must be IPv6-compliant by mid-2008. Given the number of companies that do business with the U.S. government, the federal mandate should lead to accelerated conversions in the commercial sector as well. And, as far as businesses are concerned, one of the greatest promises of IPv6 is the new platform's ability to provide a nearly limitless supply of Internet addresses.

To put things in perspective: IPv4 supports about 4.2 billion distinct Internet addresses—or fewer than one for every person on the planet. IPv6, on the other hand, supports 340 undecillion (that's 36 zeroes) addresses—more than enough to supply each grain of sand on the world's beaches with its own Internet address.

IPv6 is emerging at the same time as wireless broadband networks that necessitate an increase in IP addresses and greatly expand the practical applications for those IP addresses. This new source of Internet addresses will enable

an entire new generation of complex wireless devices, for example.

The possibilities and potential benefits of IPv6 are particularly staggering in the supply chain industry. Every package, parcel, and cargo crate could have its own unique Internet address, and wireless broadband technology will allow that address to be transmitted cheaply and easily. As a result, customers and shipping companies will be able to go online and instantly track their package to a precise location anywhere in the world, in much the same way as global positioning systems currently track vehicles on the highways. Through IPv6, these items can have their own routable Internet addresses without the need for any Internet server. This technology can vastly improve how companies track and ship cargo, providing both cost savings for companies and better service for customers.

IPv6 also has significant implications for businesses involved in the personal safety and homeland security industries. Specific information—a crash victim's medical records, for example—can be automatically collected and sent to the appropriate authorities using this new technology, similar to the way packages can be tracked when they are being shipped.

First responders such as firefighters and police departments will have faster and more reliable electronic communications with one another using an IPv6 rather than an IPv4 platform, because the "end-to-end" communications features of IPv6 are not available in IPv4. Recognizing this, the city of Harrisonburg, Va., has already implemented a municipal-wide IPv6 wireless network that substantially aids first responders in that community.

Some have speculated that an organization can obtain lower charges from its Internet service provider (ISP), because IPv6 will enable the organization to purchase fewer public Internet addresses from the ISP. Instead, the organization may use the additional addressing features of IPv6 to enable Internet communications to and from computers on the organization's internal network.

The U.S. government has set a June 30, 2008, deadline for all government agencies to be IPv6-compliant. Most federal agencies are not on track to meet that deadline, however. To date, the nation lacks a single organized effort

to implement IPv6. Representing a significant step toward expanding IPv6 compliance in the United States, Microsoft will make its newest version of the Windows operating system IPv6-compliant.

The Slow Road to IPv6 Implementation

In the United States, the federal government is a leader in conversion to IPv6. Many expect the private sector will follow the government's lead, particularly those companies that have contracts with the U.S. government, the world's largest purchaser. But so far, the switch from IPv4 to IPv6 is going more slowly than originally anticipated, which makes it more difficult to assess the privacy and data security ramifications, because the new Internet platform isn't employed in enough real-world situations.

A 2006 report by the U.S. Government Accountability Office (GAO) found that federal agencies have taken some steps in planning for IPv6 conversion, but several agencies have not yet completed important parts of the process. Many Asian nations, particularly China and Japan, have been far more aggressive in pushing along implementation of IPv6.

Ten of the 24 major agencies surveyed by the GAO still had not developed IPv6-related policies and enforcement mechanisms at the time the report was being prepared. The report's authors found that many agencies were not ready to capitalize on the advantages of IPv6, largely because they lacked incentives to use IPv6 or because they weren't far enough along in the transition process. And although 23 of the 24 agencies had at least begun an impact analysis of IPv6, only nine had assessed the costs associated with IPv6 conversion.

The federal government has set clear and laudable goals for IPv6 implementation, but so far actual conversion from IPv4 to IPv6 has fallen far short of those goals. Experts may speculate about IPv6, but its actual data security and privacy strengths and weaknesses won't be fully known until after the new platform is in widespread, day-to-day use throughout the world.

How Does IPv6 Affect the User Privacy and Data Protection Landscape?

The uncertainties of IPv6 create security concerns for both companies and individuals. The ability to collect and transmit massive amounts of data instantaneously is a blessing and a curse: Although this capacity has revolutionized how business is transacted, it also has put confidential customer and employee information at risk as it has never been before. The broader the access, the greater the risk, and IPv6 carries with it no small amount of concerns in that regard.

With its potential for stateless autoconfiguration of unique IP addresses, IPv6 can expose users to greater privacy risks. This autoconfiguration technology opens up the potential to track the same unique identifying number embedded in an IPv6 address each time a user obtains or exchanges information over the Internet. The first 64 bits of an IPv6 address describe the network and can change across connections to different networks. The second 64 bits of the IP address make up the "interface identifier," which stays the same in autoconfiguration for a particular device or host. Some have called this globally unique interface identifier "a second Social Security number."

The total of consumers' IPv4 addresses, in contrast, is only 32 bits. Often, these addresses do not have an embedded number that is constant and unique, because IPv4 technologies frequently change the IP addresses assigned to a particular computer. Organizations that collect the IP addresses of consumers may need to review their privacy notices regarding the collection of a globally constant and unique number in IP addresses of IPv6 users. If an IPv6 laptop computer is autoconfigured with a globally constant interface identifier in the IP address, geo-privacy issues arise when that computer is used in different locations—on a business trip, for example. The same interface identifier in the address can be tracked every time the traveler uses his or her laptop computer in different locations. There are some optional fixes for the IPv6 autoconfiguration privacy issues; instead of using a unique, unchanging identifying number, for example, each user can receive a periodically changing pseudo-random number.

The improved Internet platform also can be used to provide better protection for online users. The European Commission's IPv6 Task Force for the International Working Group on Data Protection in Telecommunications calls IPv6 a "potentially powerful tool to improve the possibilities of user privacy." Built-in security and privacy features of IPv6 provide protections for users that do not exist in most implementations of the current Internet Protocol. However, to be truly effective, those features must be supplemented by the user's own data security efforts.

Another security challenge is political, not technical. Governments and law enforcement agencies continue to push for greater access to personal information as part of the global war on terror. As IPv6 expands the Internet into new areas of communication, it stands to reason that law enforcement may seek greater oversight with respect to these areas as well. One commentator has recommended transition in public and private networks to IPv6 to improve tracking and tracing of IP communications for counterterrorism purposes. Law enforcement agencies will still need to grapple with the fact that IPv6 supports an optional "privacy extension" that can be used to change the interface identifier with every different connection to the Internet, making it more difficult for law enforcement to trace Internet activity to a particular computer or person.

Measures To Improve Online Security in IPv6

One major positive step is that Internet Protocol security (IPSec) is mandatory with IPv6, whereas it is only optional in IPv4. IPSec is a set of protocols designed to make sure that information "packets" are securely exchanged between computers at the IP level. The system provides the user with some protection against data theft, hacker attacks, and theft of users' credentials.

No single entity has full control of IPv6 implementation, but many of the major parties involved at least realize that privacy and data protection are real and urgent consid-

erations. In 2002, the European Commission stated, "Due to the fact that the Internet has, from the very beginning, been considered as an open network, there are many characteristics of its communication protocols, which, more by accident than design, can lead to an invasion of privacy of the Internet users. … It is therefore indispensable that the European Commission and the European Union as a whole consider privacy issues in the further development of the Internet."

The International Working Group on Data Protection in Telecommunications published a 10-point overview plan back in 1996, and its recommendations remain valid today. The group's recommendations have not and probably will not be adopted on any type of worldwide basis, but they represent a consensus of IPv6 experts and, as such, their recommendations should carry a great deal of weight during IPv6 implementation. The Working Group's 10 points are as follows:

1. Service providers should inform each potential user of the Internet unequivocally about the risks to his privacy. She will then have to balance these risks against the expected benefits.
2. In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law.
3. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of trans-border networks and services, are to be supported.
4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies. Responsibility for privacy protection will have to be institutionalized to a certain extent.
5. National and international law should state unequivocally that the process of communicating (e.g., via electronic mail) is also protected by the secrecy of telecommunications and correspondence.
6. Furthermore, it is necessary to develop technical means to improve the user's privacy on the Internet. It is mandatory to develop design principles for information and communications technology and multimedia hard[ware] and software, which will enable the individual user to control and give him feedback with regard to his personal data. In general, users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.
7. Technical means should also be used for the purpose of protecting confidentiality. The use of secure encryption methods must become and remain a legitimate option for any user of the Internet. The Working Group supports new developments of the Internet Protocol (IPv6), which offer means to improve confidentiality by encryption, classification of messages and better authentication procedures. The software manufacturers should implement the new Internet Protocol security standard in their products, and providers should support the use of these products as quickly as possible.
8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification using "quality stamps" for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.
9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.
10. Finally, it will be decisive to find out how self-regulation by way of an expanded "Netiquette" and privacy-friendly technology might improve the implementation of national and international regulations on privacy protection. It will not suffice to rely on any one of these courses of action: they will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.

You may say: That's all fine, but what should *my* organization be doing to address IPv6 privacy and security issues? Here is a starter list:

1. Understand the new technology capabilities of IPv6 and make a business decision about whether, when, and how your organization will implement IPv6 or become IPv6-ready. The European Union is aggressively supporting IPv6 to achieve a global competitive advantage.
2. Understand the security-enhancing features of IPv6 as well as the features of IPv6 that raise new challenges to the security of data. Design and build IPv6 security in your network from the beginning; you have a fresh start (as opposed to the current environment of 20 years of IPv4 security patches and add-ons).
3. Understand and address the security challenges in transitioning from IPv4 to IPv6. Even if you move your entire organization to IPv6, your trading partners and the rest of the world will not all move to IPv6 at the same time that your organization does. IPv6 clients (for example, personal computers) in your organization will still need to communicate with the outside world.
4. Understand and address the security threats to your organization's IPv4 network devices (such as firewalls, routers, and the like) and clients from incoming IPv6 traffic that exists today. Even if you decide that you do not need to transition your systems to IPv6 in the foreseeable future, hackers are already using IPv6 technologies to attack IPv4 systems. For example, unless a system administrator implements proper protective controls, an attacker may be able to send IPv6 malicious code through an IPv4 "tunnel" and install backdoor programs on an IPv4 host or client that do not show up in IPv4 security scans. Also, IPv4 firewalls may need to be specifically configured to recognize and filter IPv6 traffic.
5. Make sure you identify IPv6 clients who may be ac-

cessing your network without your knowledge. For example, an employee may connect a personal computer with Windows Vista™ software to your network. Because Windows Vista is shipped with IPv6 "default on," through IPv6, the program could be revealing its site-local address within your network to outsiders, thus exposing the computer to new threats by attackers. Also, users can easily self-install IPv6 in computers that have Windows XP™ software installed, and in some network configurations the network administrator will not be able to detect the IPv6 installation.

6. Incorporate IPv6 security risk management into your supply chain processes. Do this for technology acquisitions and also to protect against vendors and business partners who have access to the organization's sensitive information, including trade secrets and sensitive personally identifiable information. Just as your own organization needs to manage IPv6 security challenges in its own systems, your organization should address how its vendors are addressing IPv6 in their systems.
7. IPv6 calls for a fundamental re-evaluation of basic information security models. In IPv4 networks, the "perimeter defense" concept prevails; this means there are protective firewalls, gateway routers, internal routers, and other devices that stand between the Internet and the network's hosts and clients (personal computers, for example). In contrast, the "plug-n-play" nature of some IPv6 implementations can mean that there is a virtual network that is distributed beyond an organization's "perimeter." There is no perimeter firewall; distributed devices have their own individual firewalls. According to Tom Patterson, chief executive officer of Command Information, an IPv6 consulting and testing company, "In short, if you proactively address IPv6 security, you can get more security for a lot less money. Conversely, if you ignore the security changes that come with IPv6, you'll end up with a lot less security for a lot more money."

Conclusion

Internet Protocol Version 6, should not be considered a magic bullet that ensures user privacy any more than it should be looked upon as a step backward for data protection. Instead, IPv6, like the current Internet Protocol, provides both opportunities and challenges for information privacy and protection. The onus ultimately will remain on administrators and users of IPv6 technology to ensure that data related to their employees, customers, and clients are stored and transmitted securely.

Michael W. Hubbard is the leader of Womble Carlyle's Privacy and Data Protection Team and practices in the firm's office in Raleigh, N.C.

References

(All sites last visited on Aug. 9, 2007)

Comments before the National Institute of Standards and Technology (March 8, 2004), www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/comments/EPIC_IPv6.htm.

Communication from the Commission to the Council and the European Parliament, *Next Generation Internet Priorities for Action in Migrating to the New Internet Protocol IPv6* (2002), eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002DC0096:EN:HTML.

Convery, Sean, and Darrin Miller. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v 1.0)* (2004), www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf.

Davies, Joseph. *IPv6 Improvements in Windows Vista*, 6Sense Newsletter (2006), www.usipv6.com/6sense/2006/apr/01.htm.

International Working Group on Data Protection in Telecommunications. *Draft Report and Guidance on Data Protection on the Internet* (May 1996), trout.cpsr.org/cpsr/lists/rre/Data_Protection_and_Privacy_on.

Kaisor, Basar, et al. *IPv6: Legal Aspects of the New Internet Protocol* (Euro6IX, 2005), www.ipv6tf.org/pdf/ipv6legalaspects.pdf.

Marsan, Carolyn Duffy. *Windows Vista Not Playing Well with IPv6*, PCWorld (2007), www.pcworld.com/article/id,132689-c,vistalonghorn/article.html.

National Telecommunications and Information Administration. *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (January 2006), www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final.pdf.

U.S. Government Accountability Office. *Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain* (June 2006), www.gao.gov/new.items/d06675.pdf.

Warfield, Michael H. *Security Implications of IPv6*, Internet Security Systems 2003, documents.iss.net/whitepapers/IPv6.pdf.

Westby, Jody R. *Countering Terrorism with Cyber Security* at 14 (August 2006), www.cyberconflict.org/pdf/JodyWestby-WFS-TerrorismFlourishesPaperv6.pdf.

The Federal Trade Commission's Expansion of the

By Benita A. Kahn and Heather J. Enlow

Data breaches are receiving increasing exposure and media attention as the list of those affected, the amount of information compromised, and the costs to the compromised company rapidly increase. In January, TJX announced the largest data breach to date, with over 45 million credit cards compromised. Additionally, according to the Privacy Rights Clearinghouse, over 159 million records containing the sensitive personal information of U.S. residents have been involved in data breaches since January 2005. As this problem has continued to grow, the FTC has stepped in to "protect" consumers. This article explores the evolution of the FTC's use of its jurisdiction to address these data breaches and questions whether the FTC has expanded its jurisdiction beyond its authority under the FTC Act.

Data breaches exposing thousands and even millions of consumers' personal financial information collected by large U.S. retailers, agencies, and universities seem to grace the headlines daily.[1] You may have even received a letter in the mail stating that your credit card or debit card number and/or other personal information—such as your driver's license number—had been compromised. In January 2007, TJX Companies Inc. announced the largest data breach to date: a breach that involved more than 45 million credit cards and debit cards used at the company's stores.[2]

Many lawsuits have been filed against TJX as a result of this breach, and the Federal Trade Commission (FTC) has announced that it is investigating TJX as well.[3] This article will explore how the FTC has used its § 5 authority in the wake of several high-profile data breaches. First, this article will discuss § 5 authority generally and then look at the FTC's authority under the Gramm-Leach-Bliley Act (GLBA), its resulting Safeguards Rule, and the FTC's expansion of the Safeguards Rule in actions against nonfinancial institutions involved in data compromises. Finally, the article will compare the FTC consent orders entered into with the retailers in the data breach context to litigation involving those data breaches. The discussion will conclude by questioning whether the FTC has indeed met its requirements for jurisdiction in these types of cases.

FTC Jurisdiction

The FTC's ∫ 5 Authority

The Federal Trade Commission Act, 15 U.S.C. §§ 41, *et seq*. (2007), prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1) (2007). The FTC Act was initially enacted to prohibit unfair methods of competition in commerce and to supplement and bolster the Sherman and Clayton Acts.[4] The act was also intended to condemn existing violations of the Sherman and Clayton Acts as unfair methods of competition.[5] Since it was enacted, the FTC Act has been amended to outlaw unfair or deceptive acts or practices in commerce, so that the Federal Trade Commission can take steps to directly protect consumers, not just business competitors.[6]

The FTC is one of the primary federal regulators of retail merchants. Section 5 of the FTC Act invests the FTC with broad investigative powers to determine unfair and deceptive trade practices that affect consumers. The FTC is also empowered to initiate federal court actions in order to enforce violations of § 5 and to seek appropriate equitable relief. 15 U.S.C. § 53(a)-(b), 57(b) (2007). Under this general enforcement authority, the FTC can investigate and pursue actions against businesses whose activities qualify as practices that "cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n) (2007).

FTC Jurisdiction Under the Gramm-Leach-Bliley Act

Under the Gramm-Leach-Bliley Act, "financial institutions" have an affirmative and continuing obligation to address the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information. 15 U.S.C § 6801(a) (2007). With respect to the security requirements under GLBA, the act requires financial institutions to: (1) establish appropriate standards for administrative, technical, and physical safeguards that will ensure the security and confidentiality of customer information; (2) protect the security of these records against any anticipated threats; and (3) protect customers against unauthorized access or use of this information, which could result in substantial harm or inconvenience to customers. 15 U.S.C. § 6801(b) (2007).

The term "financial institutions" is broadly defined under GLBA and includes institutions that are significantly engaged in financial activities. Examples of financial institutions other than the obvious banks and savings and loan institutions include mortgage brokers, check cashing businesses, and car dealers that arrange for the financing or leasing of a personal car. 16 C.F.R. § 313.3(K)(2) (2007). Because of the breadth of the definition of financial institutions, many of the "financial institutions" covered by GLBA do not have a specified regulator such as the Office of the Comptroller of the Currency or the Federal Deposit Insurance Corporation. As a result, the FTC is granted specific jurisdiction to regulate these entities and is responsible for enforcing the safeguard provisions included in the act. As required by GLBA, the FTC implemented the Safeguards Rule to set forth the standards for the protection of customer records and information that are to be followed by the financial institutions that the FTC regulates.

The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the institution's size and complexity, the nature and scope of activities, and the sensitivity of any customer information at issue. *See* 16 C.F.R. § 314 (2007). These requirements include the following:

- designating someone to coordinate the information security program;
- performing a risk assessment that considers personnel training, information systems, and the detection, prevention, and response to attacks, intrusions, and other systems failures;
- designing and implementing safeguards to control risks and regularly testing safeguards to monitor effectiveness;
- overseeing service providers by ensuring that they are able to take appropriate security precautions and in fact do so; and
- updating the security program as necessary in response to frequent monitoring and material changes in the business.

According to an FTC official, "An actual breach of security is not a prerequisite for enforcement under § 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate."[7]

The Expansion of FTC Actions Against Nonfinancial Institutions

GLBA defines financial institution broadly, but the act generally does not cover retail merchants that do not issue their own credit. However, over the past several years the FTC has embarked on an aggressive strategy of investigations and has threatened enforcement actions against companies that had their customers' nonpublic personal information stolen through asserted data compromises. These investigations have resulted in companies not subject to GLBA to effectively agree to implement the Safeguards Rule and to submit to independent security audits for a set period of time—usually 20 years.

In early enforcement actions against these nonfinancial institutions, the FTC relied on the deception aspect of § 5 of the FTC Act. The FTC asserted that the privacy statements of companies contained false and misleading information in light of subsequent security breaches. One such case was that of Petco Animal Supplies Inc. Petco's online privacy policy stated that Petco encrypted consumers' personal information both in transit and in storage. After the online theft of customers' credit card information, however, it was determined that Petco did not encrypt customers' credit card information when stored.

Petco settled the FTC's charges that a security flaw in its Web site allowed hackers to access consumer records,

including credit card numbers. The FTC alleged that had Petco actually encrypted the data as promised, the credit card information would not have been accessed. The FTC stated that the false promises Petco had made to consumers were deceptive and therefore violated § 5 of the FTC Act. As part of the settlement, Petco agreed to establish and maintain a comprehensive security program that mirrors the requirements of the Safeguards Rule. The settlement also required biennial audits of the company's security program by an independent third party for the next 20 years, and required Petco to maintain records so that the FTC may monitor compliance.[8]

Subsequent data compromises occurred in stores, rather than on Web sites, and the FTC could not rely on deceptive privacy policies as a basis for enforcement actions. Therefore, the FTC turned to the FTC Act's unfairness doctrine to pursue enforcement. Unfairness under the FTC Act has three specific elements: (1) the violation causes substantial injury to consumers; (2) consumers are unable to reasonably avoid the injury; and (3) the substantial injury is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n) (2007). By using the unfairness doctrine, the FTC has expanded the reach of the Safeguards Rule beyond financial institutions, extending it to nonfinancial institutions that experience security breaches, by asserting that these entities did not have reasonable information security policies and procedures in place. The question that is raised, however, is whether the FTC can meet all these standards in a case that is litigated.

The first instance of the FTC's expansion of the Safeguards Rule occurred in the consent order entered into with BJ's Wholesale Club. Between July 2003 and February 2004, unauthorized persons accessed BJ's computer systems as well as the credit card and debit card numbers of thousands of customers. Visa discovered this security breach and notified BJ's and the banks within the Visa network. In the investigation and enforcement action against BJ's, the FTC pursued the broader strategy of alleging that the failure to ensure adequate security measures constituted an unfair practice. The commission did not claim that BJ's had made misrepresentations to its customers, as the FTC did in the Petco action. Rather, the FTC alleged that the failure of BJ's to provide adequate security measures constituted an unfair practice that violated federal law. The unreasonable security measures asserted by the FTC included the following actions by BJ's:

- failure to encrypt personal data while in transit or when stored on the computer networks of their stores;
- creation of unnecessary risks by storing information longer than necessary in violation of bank rules;
- storage of personal data in easily accessible files;
- failure to take adequate steps to prevent unauthorized wireless connections; and
- failure to take reasonable measures to detect unauthorized network access and failure to conduct security audits.

In the consent order, BJ's essentially agreed to implement the requirements of the FTC's Safeguards Rule and to perform biennial security audits for the next 20 years.[9]

Relying on the unfairness doctrine, these same Safeguards Rule standards and audit requirements have been imposed in a subsequent settlement by a merchant with the FTC stemming from the theft of credit card information.[10] These merchant settlements have resulted in the expansion by the FTC of the Safeguards Rule beyond the financial institutions the FTC regulates under GLBA to nonfinancial institutions such as retail merchants. The standard has required the retail merchants to implement a comprehensive information security program and biennial audits by an independent third-party security professional for 20 years. However, financial institutions that have violated GLBA receive lesser terms.[11] Because these FTC investigations resulted in settlements rather than litigated enforcement, no court has made a determination of whether the FTC can meet all the requirements of the unfairness standard when a retail merchant is involved in a data compromise of customer information. The decisions in ongoing civil litigation against these merchants, however, may shed some light on the FTC's ability to meet all the elements of the unfairness doctrine.

Data Breach Litigation

To date, courts have rarely adjudicated favorably the claims of plaintiffs whose nonpublic personal information has been lost or stolen. In fact, in the data breach context, courts have frequently held that plaintiffs have not suffered injuries-in-fact, reasoning that an increased risk of identity theft is insufficient to support the injury-in-fact requirement of Article III standing.[12] Moreover, this alleged injury of an increased risk of future harm has been judged insufficient to support the damages requirements of tort actions and contract claims.[13] Courts have noted the danger in awarding damages to buy "peace of mind" as well as the possibility that plaintiffs could conceivably be awarded damages not only in the present for a perceived increased risk of harm but also in the future, if and when actual harm occurs.[14]

Specifically, in cases against merchants, the courts have ruled against the plaintiffs for lack of injury. In *Key v. DSW Inc.*, the plaintiff alleged that because of DSW's data breach, she had been subjected to a substantially increased risk of identity theft or other financial crimes. In dismissing all claims, the court held that the plaintiff lacked Article III standing. "To satisfy the case or controversy requirement a plaintiff must establish three elements: '(1) an injury-in-fact that is concrete and particularized; (2) a connection between the injury and the conduct at issue—the injury must be fairly traceable to the defendant's action; and (3) likelihood that the injury would be redressed by a favorable decision by the Court.'"[15] Under this standard, a plaintiff's injury must be "actual or imminent," and not "conjectural or hypothetical."[16]

The court held that a substantial increased risk of identity theft or other related financial crimes was insufficient to confer standing to sue. Reasoning that, in the identity theft context, courts have held an alleged increase in risk of future injury is not an actual or imminent injury, the court

held the plaintiff's injury was not actual or imminent.

> At the present time, Plaintiff has not alleged evidence that a third party intends to make unauthorized use of her financial information or of her identity. The mere inquiry as to who would cause harm to Plaintiff, when it would occur, and how much illustrated the indefinite, and speculative nature of Plaintiff's alleged injury. In sum, Plaintiff's claims are based on nothing more than a speculation that she will be a victim of wrongdoing at some unidentified point in the indefinite future. Because Plaintiff has failed to allege that she suffered injury-in-fact that was either 'actual or imminent,' this Court is precluded from finding that she has standing under Article III.[17]

Even when there is evidence of fraudulent use of an individual's credit cards and debit cards, that individual is not held responsible for those purchases under many banks' Zero Liability Policies.[18] Courts, therefore, have been reluctant to state that fraudulent use of a credit or debit card constitutes an injury when there was no actual injury. Plaintiffs have also run into causation problems. For example, in *Stollenwerk v. Tri-West Healthcare Alliance*, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005), one plaintiff's identity was actually stolen, costing that person thousands of dollars. However, the plaintiff could not prove that the defendant's data breach was the proximate cause of his identity theft, and the court granted judgment to defendant. Thus, courts have been reluctant to rule favorably for plaintiffs in the data breach context, because they are unable to identify cognizable damages.[19]

Conclusion

In conducting its investigations of data breaches, the FTC has claimed a violation of the unfairness doctrine. In the consent orders imposed on retailers involved in data compromises, the FTC stated that it had jurisdiction, because the "failure to secure customers' sensitive information was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition."[20]

It is interesting that, given the same set of facts, courts have failed to recognize asserted claims or the existence of injuries to allow banks or consumers to recover against an entity that has suffered a data breach. The courts found that an alleged increase in risk of future injury is not an actual or imminent injury—much less a substantial injury. Along with court rulings, the implementation of the Zero Liability Policy issued by credit card associations to protect consumers against all liability resulting from fraudulent transactions on their credit or debit cards addresses the issue of consumers' ability to reasonably avoid any potential injury when credit card information is compromised. Moreover, findings in a report released by the Government Accountability Office in June 2007 raise further questions as to whether the unfairness test can be met.[21] The report stated that research through interviews and data "indicated that most breaches have not resulted in detected incidents of identity theft" and that there is great difficulty in determining the source of the data used to commit identity theft.[22]

If the anticipation or perceived risk of future harm is insufficient to meet the requirements of injury-in-fact for standing, can this same perceived risk from a data compromise of credit card information, for which consumers can avoid injury through reporting, be sufficient to meet the requirements of the unfairness doctrine? One must wonder if § 5 of the FTC Act was meant to be used in this way. **TFL**

Benita A. Kahn, a partner with Vorys, Sater, Seymour and Pease LLP in its Columbus, Ohio, office, specializes in privacy, data security, and consumer protection laws and represents numerous national retail clients. Heather J. Enlow, an associate with Vorys, Sater, Seymour and Pease LLP in the same office, provided significant assistance in preparing this article.

Endnotes

[1]For a complete list of security breaches since 2005, see Privacy Rights Clearinghouse, *Chronology of Data Breaches*, April 22, 2007, available at www.privacyrights.org/ar/ChronDataBreaches.htm.

[2]*See TJX Companies Inc.*, 10-K, March 28, 2007, available at ir.10kwizard.com/files.php?source=487.

[3]As of March 2007, 16 lawsuits have been filed against TJX as a result of the data breach announced in January. *See id.* More recent reports indicate that to date 19 lawsuits have been filed.

[4]*See generally FTC v. Beech-Nut Packing Co.*, 257 U.S. 441 (1992); *Luria Bros. & Co. v. FTC*, 389 F.2d 847 (3d Cir. 1968).

[5]*See generally FTC v. Brown Shoe Co.*, 384 U.S. 316 (1966).

[6]*See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972); *FTC v. A.P.W. Paper Co.*, 328 U.S. 193 (1946). In spite of this broad jurisdiction to protect consumers, the FTC Act excludes some industries from its jurisdiction, such as banks, savings and loan institutions, common carriers, air carriers, and others. 15 U.S.C. § 45(a)(1) (2007).

[7]Deborah Platt Majoras, FTC chair, "Data Breaches and Identity Theft," Testimony before the Senate Committee on Commerce, Science, and Transportation, 109th Cong. 6 (June 16, 2005), available at commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Testimony&Hearing_ID=1536&Witness_ID=3484.

[8]FTC, Press Release, "Petco Settles FTC Charges: Security Flaws Allowed Hackers to Access Consumers' Credit Card Information" (Nov. 17, 2004), available at www.ftc.gov/opa/2004/11/petco.htm.

[9]FTC, Press Release, "BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards" (June 16, 2005), available at www.ftc.gov/opa/2005/06/bjswholesale.shtm.

[10]FTC, Press Release, "DSW Inc. Settles FTC Charges: Agency Says Company Failed to Protect Sensitive Customer Data" (Dec. 1, 2005), available at www.ftc.gov/

opa/2005/12/dsw.shtm.

[11]*See In the Matter of Nationwide Mortgage Group Inc. and John D. Eubank*, File No. 042-3104, Agreement Containing Consent Order (March 4, 2005), available at www.ftc.gov/os/adjpro/d9319/index.shtm; *see also In the Matter of Sunbelt Lending Services Inc.*, File No. 042-3153, Agreement Containing Consent Order (Nov. 16, 2004), available at www.ftc.gov/os/caselist/0423153/04231513.shtm. Both Nationwide Mortgage Group and Sunbelt Lending Services were required to implement biennial auditing for only 10 years.

[12]*See Randolph v. ING Life Ins. and Annuity*, No. 06-1228 (CKK), 2007 WL 565872 (D. D.C. Feb. 20, 2007) (plaintiffs failed to allege a cognizable injury-in-fact where the laptop computer of the defendant was stolen containing plaintiffs' personal information but there was no evidence the information had been accessed or improperly used); *Bell v. Acxiom Corp.*, No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (plaintiff lacked standing because she failed to allege she had suffered concrete damages where defendant's computer files were improperly accessed; assertions of potential future injury do not satisfy injury-in-fact requirement); *Key v. DSW Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006) (plaintiff lacked standing because her alleged increase in risk of future harm was insufficient to show injury-in-fact where defendants' computer systems had been improperly accessed; court also found future risk was insufficient for cognizable damages for contract, negligence, conversion, and fiduciary duty claims); *Giordano v. Wachovia Securities LLC*, No. 06-476, 2006 WL 2177036 (D. N.J. July 31, 2006) (defendant lost a backup tape containing the plaintiff's personal information but the court concluded that the mere possibility of future harm fails to satisfy the standard of concrete and particularized harm).

[13]*See Kahle v. Litton Loan Servicing LP*, 486 F. Supp. 2d 705 (S.D. Ohio 2007) (plaintiff's choice to purchase credit monitoring services and an alleged increased risk of future harm was insufficient to support the damages element of her negligence claim where there was no evidence her information was accessed or used for identity fraud); *Hendricks v. DSW Shoe Warehouse Inc.*, 444 F. Supp. 2d 775 (W.D. Mich. 2006) (plaintiff failed to allege cognizable damages where she did not allege her personal information had been used or her credit damaged); *Forbes v. Wells Fargo Bank*, 420 F. Supp. 2d 1018 (N.A.D. Minn. 2006) (plaintiff's perceived risk of future harm was insufficient to satisfy the damages requirements where computers containing unencrypted personal information were stolen from the defendant's service provider); *Guin v. Brazos Higher Educ. Serv. Corp. Inc.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006) (plaintiff could not establish he suffered any injury to support his negligence claim against the defendant where a laptop computer belonging to the defendant was stolen from an employee's home).

[14]*Hendricks*, 444 F. Supp. 2d at 779–780.

[15]*Key*, 454 F. Supp. 2d at 686-687 (citing *Courtney v. Smith*, 297 F.3d 455, 459 (6th Cir. 2002)); *see Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); *Allen v. Wright*, 468 U.S. 737, 751 (1984).

[16]*Key*, 454 F. Supp. 2d at 687 (quoting *Lujan*, 504 U.S. at 560).

[17]*Id.* at 690.

[18]*See, e.g., Banknorth v. BJ's Wholesale Club Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006) (noting that the plaintiff bank's equitable subrogation claim failed because, under its Zero Liability Policy, the customer is not held liable for fraudulent purchases).

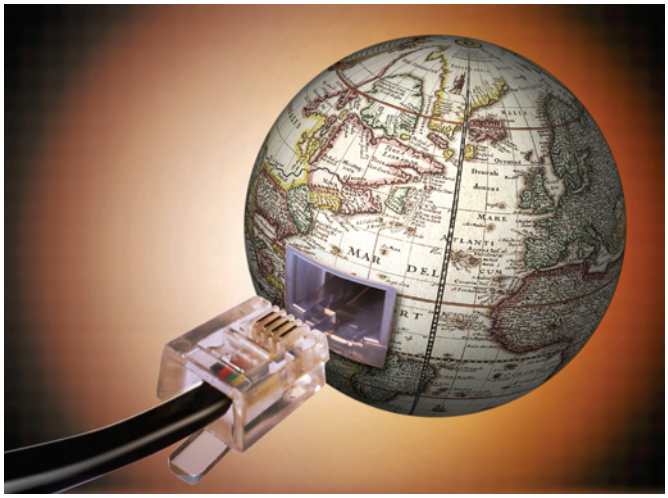
[19]Note that, in the rare cases in which the courts have ruled in favor of plaintiffs, the plaintiffs had suffered actual financial harm and were able to prove who stole their identities. *See Bell v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees, AFL-CIO, Local 1023*, No. 246684, 2005 WL 356306 (Mich. App. Feb. 15, 2005) (where the daughter of the union's treasurer had stolen the identities of several members, and the court upheld the jury award against the union, finding that the union had a duty to safeguard its members' nonpublic personal information); *Daly v. Metropolitan Life Ins. Co.*, 4 Misc.3d 887 (N.Y. 2004) (where two employees of the defendant had accessed the plaintiff's nonpublic personal information and used the information to establish and use numerous credit accounts; the court held that the defendant had a duty to protect the plaintiff's nonpublic personal information); *see also Jones v. Commerce Bankcorp. Inc.*, No. 05-5600 (D. N.J. July 16, 2007) (court certified settlement class and approved settlement where five employees stole customer information and sold it to a criminal; police had arrested the employees and the criminal, finding the confidential banking information of numerous Commerce customers in their possession).

[20]FTC, Press Release, "DSW Inc. Settles FTC Charges"; *see also* FTC, Press Release, "BJ's Wholesale Club Settles FTC Charges."

[21]U.S. Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, GAO-07-737 (June 4, 2007), available at www.gao.gov/docsearch/abstract.php?rptno=GAO-07-737.

[22]*Id.* at 5.

Data Protection Law in the *European Union*



European data protection law is vastly different from U.S. privacy law, regulating virtually all information about individuals, applicable to all industry types, and taking a much more expansive view of the types of activities that should be controlled and restricted. The consequences for violating these laws, which can include injunctions that interfere with business activity and criminal penalties, are also notably different from U.S. penalties, which tend to be limited to relatively modest monetary sanctions. If your company or client does business with or employs EU residents, this article will help you identify whether EU data protection compliance is something you need to address.

By Elizabeth H. Johnson

The European Union established the first legal system in the world to produce a comprehensive, omnibus approach to privacy and data protection. The legal regime established in the EU is unique because of its expansive nature, featuring active oversight and enforcement of complex laws and regulations that cover all industry sectors and all types of data processing.

The strict and comprehensive nature of EU data protection law stems from the European experience in World War II, when personal information was collected and used for the purpose of genocide. As a result, the philosophical underpinnings of EU data protection law contrast greatly with those of U.S. privacy law, which tends to focus on preventing identity theft and fraud. Conversely, EU data protection law tends to offer much broader coverage and is more restrictive in the limitations it imposes.

Europe's sad history with respect to the abuse of personal information has led Europeans to treat data protection as a fundamental human right. The laws protecting this right can be traced to human rights treaties and various national constitutions. In a groundbreaking judgment rendered in 1983, the German Federal Constitutional Court recognized a "right to informational self-determination," which is also recognized in various human rights treaties concluded by European nations.

The EU currently consists of 27 European nations, or member states. To govern this coalition of states, EU government bodies produce legal frameworks known as directives, which member states are then required to implement by enacting and enforcing codifying legislation. Because member states' laws may vary in the way they implement EU directives, compliance with EU data protection law requires understanding both the relevant directives and the variations of each particular member state's enabling legislation.

Because the EU issues directives, EU data protection law has several key features that are common in each member state, including the creation of a minimum level of data protection for individuals and the elimination of restrictions on data transfers among EU member states (recognizing that implementation of directives related to data protection ensures the minimum level of protection). Compliance with these requirements is interpreted and enforced by national regulatory bodies referred to as data protection authorities (DPAs). Private entities often complain that the rules of EU data protection law are overly bureaucratic (for example, rules on registering databases with DPAs), inflexible and burdensome (for example, rules governing international transfers of data), and difficult to follow because individual nations' interpretations of these requirements can vary widely. The lack of harmonization among member states is one of the primary criticisms levied against the EU model of data protection.

Introductory Concepts

The EU's data protection law is replete with its own terminology, which can often make the rules difficult to understand. One of the most important terms is "personal data," which is the information safeguarded by EU data protection law. "Personal data" are defined as "any information relating to an identified or identifiable natural person. An "identifiable person" is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the person's "physical, physiological, mental, economic, cultural or social identity." Obviously, the concept of personal data is quite broad and includes almost any type of data that can be traced to an individual. Although U.S. entities are often concerned only with compliance as it pertains to information about customers, the broad European definition of personal data requires private entities to consider

compliance with respect to the personal data of their employees, customers, suppliers, vendors, and other contacts. These individuals, whose personal data receive the legal protections discussed herein, are referred to as "data subjects." Any individual residing in the EU or whose personal data are processed in the EU is potentially a data subject.

The term "data processing" is also significant and further broadens the scope of EU data protection law. "Data processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Again, this term is quite broad, encompassing virtually any use of personal data, including mere collection. Related concepts include "data controllers," that is, the entities that have the authority to determine how personal data are processed (usually the business that "owns" the data), and "data processors," that is, the third parties that process personal data at the direction of data controllers. Data processors may have significant access to personal data and may even collect it for data controllers.

Legal Instruments and Basic Principles

EU data protection law is governed primarily by three directives: (1) the General Directive, (2) the Directive on Privacy and Electronic Communications, and (3) the Directive on Data Retention. As discussed above, each EU member state is required to enact national laws that give force and effect to these directives.

General Directive

The major instrument of EU data protection law is the Data Protection Directive, or "General Directive, which was adopted on Oct. 24, 1995. The General Directive is founded on six primary principles:

1. Legitimacy: Personal data may only be processed for limited, legitimate purposes.
2. Finality: Personal data may be collected only for specified, legitimate purposes and may not be further processed for any incompatible purpose.
3. Transparency: Data subjects must receive information about the processing of their personal data.
4. Proportionality: Personal data must be relevant and not excessive in relation to the purpose for which they are collected and processed.
5. Confidentiality and security: Technical and organizational measures appropriate to the risks presented by the data processing must be in place to ensure the confidentiality and security of personal data.
6. Control: Data protection authorities must enforce data protection law.

Under the General Directive, personal data may be used only for the purposes to which the individual has consented or for purposes that would be reasonably obvious to the individual on the basis of the information provided at the time the data were initially collected. Explicit consent is virtually always required when the personal data are deemed "sensitive," defined as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning the person's health or sex life. Some member states also view criminal histories or driving records as sensitive personal data.

Data subjects must be provided with certain information when their data are collected for processing, including the following:

- the identity of the entity processing the data;
- confirmation that their data will be processed and the purposes of the processing;
- the categories of data concerned and the recipients or categories of recipients to whom the data will be disclosed;
- the logic involved in any automatic data processing; and
- the subject's right to request rectification of inaccurate data and erasure or blocking of data processing that does not comply with the directive.

Directive on Privacy and Electronic Communications

The Directive on Privacy and Electronic Communications addresses data protection in the electronic communications sector, which includes telecommunications, faxes, e-mail, the Internet, and similar services. Specifically, this directive applies to personal data processed in publicly available electronic communications services in public communications networks in the community. Providers of such services must take appropriate technical and organizational measures to safeguard their systems and services. Member states are required to ensure the confidentiality of communications by national legislation, though limited exceptions are provided when government wiretapping activities and national security interests necessitate disclosure. Among other provisions, the processing of traffic and billing data is subject to further restrictions. In particular, subjects of data searches are given specific rights with regard to itemized billing, calling line identification, call forwarding, directories, and unsolicited calls.

Data Retention Directive

In the EU, member states often obligate providers of publicly available electronic communication services to retain certain data—primarily communications traffic data—to ensure that such data are available for law enforcement, national security, and related purposes. The Data Retention Directive attempts to harmonize the various retention requirements imposed by member states. The directive requires telecommunications companies to retain a wide range of data, including incoming and outgoing telephone numbers (fixed and mobile), the duration of the calls, addresses of Internet providers (dynamic and static), log-in and log-off times, and e-mail activity. Member states can decide for themselves how long data should be retained

within a minimum of six months and a maximum of 24 months from the date of communication, but the data must be erased after this time. Processing of the data during the retention period must be carried out in accordance with the requirements of the General Data Protection Directive, which member states must implement by Sept. 15, 2007.

Practical Implications

EU data protection law has important practical implications for companies conducting business in the region. For instance, the transparency principle mandates that companies must notify all data subjects (customers, employees, and so forth) of the types of personal data collected, the purposes for which they are processed, and the categories of recipients to whom the data may be disclosed. In addition, the proportionality principle requires companies to consider carefully the types of personal data necessary for the companies' purposes and to limit their collection to only those data. The most significant and burdensome of the EU data protection requirements are discussed below.

Data Processing Registrations

Companies doing business in the EU are often required to notify data protection authorities of the companies' data-processing activities, whether the firms conduct these activities themselves or contract with a service provider to do so. Most member states prescribe a registration procedure by virtue of which each DPA must be notified of any database containing personal data. The DPA may use specific application forms for this procedure, and the form and scope of the forms vary widely among member states. For example, registrations in the United Kingdom are often only a page or two in length, whereas the application form used in Italy is 86 pages long. The process is further complicated by the typical requirement that these forms be submitted in the local language. Despite wide variations among member states, the registration usually entails providing a contact person and describing the type of personal data processed, data subjects affected, purposes of the processing, security applied to the data, and any transfers or disclosures of the data.

Article 18(2) of the General Directive allows member states to create exceptions to the registration requirement. However, although some nations do provide such exceptions, this practice is hardly uniform. One of the more common exceptions applies when a company appoints a data protection officer to safeguard personal data processed by or on behalf of the company. The laws of France, Germany, Luxembourg, Sweden, and the Netherlands provide for such an exception. Usually, the company must notify the DPA of the data protection officer's appointment, and that officer is required to keep inventories of the data processing activities that would otherwise have been registered with the DPA. These inventories could, in principle, be reviewed by the DPA in the event of an inspection. The company must ensure that, if the data protection officer is to have other job responsibilities, these must not conflict with the responsibility to uphold EU data protection principles.

International Data Transfers

Among the restrictions of greatest importance to companies are those pertaining to the international transfer of personal data. Personal data may not be transferred to countries outside the EU unless there is a "legal basis" for the transfer. Several possible grounds may provide a legal basis to transfer personal data to a non-EU country. First, the European Commission may issue an official "adequacy finding," determining that the country in question offers an adequate level of data protection on the basis of its national laws. Since the enactment of the General Directive, the European Commission has issued only a very small number of adequacy determinations; these cover Argentina, Canada, Guernsey, the Isle of Man, and Switzerland.

There are several other potential legal bases for international data transfers when the country to which personal data will be sent has not received an adequacy finding. The most important such legal bases are the following:

- The consent of the individual whose data are being transferred: Consent can be difficult to manage in practice, however, because consent may be revoked. In addition, consent is not always considered legally valid, particularly in the employment context, in which consent is sometimes viewed as coerced.
- Execution of the EU-approved "standard contractual clauses": These standardized data transfer agreements are concluded between the "data exporter" (the entity in the EU) and the "data importer" (the entity outside the EU), which agree to grant certain protections to the data. The clauses have been given an adequacy finding by the EU and therefore may not be modified by the signing parties; rather, the parties are required to describe the nature of their data transfer in an annex to the clauses. Some countries require the executed clauses to be filed with the DPA, and several require affirmative approval from the DPA prior to the transfer. As such, the clauses are difficult to use in practice, particularly when a company seeks to transfer personal data to hundreds of its subsidiaries worldwide, because each of these entities would be required to execute the clauses.
- The transfer is necessary for the performance of a contract between the entity transferring the personal data outside the EU and the individual whose data are being processed: This legal ground is construed strictly and is useful only in certain narrowly defined situations (for example, when a person in Europe books a hotel for a foreign vacation and needs to transfer data about his or her stay to the hotel outside the EU).
- The U.S. Safe Harbor program: This program is a voluntary, self-regulatory scheme that has received an adequacy finding from the European Commission. Companies choosing to join the program must certify their compliance on an annual basis. The program is available only to entities subject to Federal Trade Commission jurisdiction; therefore, the program only provides a legal basis for transfers of personal data from the EU to entities that have been certified as safe harbors in the

United States.

- Implementation of "Binding Corporate Rules": Binding corporate rules are a set of data processing rules and principles adopted by a company that bind all of the company's entities worldwide to certain data protection requirements. These rules must be approved by DPAs but, once approved, allow the legal international transfer of personal data among the entities bound to comply with the binding corporate rules. Through the use of these rules, the entire corporate group essentially becomes a "safe haven" in which personal data can be freely transferred from one corporate member to another, receiving the same protection wherever the data are sent and shifting the burden of ensuring compliance to companies themselves.

Because many companies in Europe spend considerable time and money complying with the EU law's restrictions on international data transfers, the regulations have significant economic implications. The restrictions can have particularly serious consequences for outsourcing transactions, because a company in Europe may not transfer personal data for outsourcing purposes to, for example, China or India, without first identifying one of the specific valid legal bases for the transfer, as discussed above. This often adds considerable cost and complexity to outsourcing transactions.

Direct Marketing

The Directive on Privacy and Electronic Communications directs member states to allow unsolicited commercial telephone calls, e-mails, and faxes only with the prior consent of the recipient. Two types of consent are recognized in the EU: "opt-in," or explicit, consent is obtained when the data subject affirmatively indicates his or her preference to receive marketing communications; and "opt-out" consent is obtained when the data subject is presented with an opportunity to object to receiving marketing communications but does not do so.

The media by which marketing communications are sent will dictate the form of consent required. Though the requirements vary by member state (as with most areas of EU data protection law), opt-in consent usually is required prior to sending faxes or placing telephone calls. Opt-in consent also is typically required prior to sending unsolicited e-mail communications. An exception is made for marketing e-mails sent to data subjects with whom a company already has an "existing business relationship." In that circumstance, the company is considered to have obtained "soft opt-in" consent from the data subject if the contact information was obtained in the course of a sale, contracting, or negotiations and the proposed communication pertains to products and services similar to those that were the subject of the existing business relationship. Regardless of the type of consent obtained at the outset, every direct marketing message sent subsequently must contain a mechanism to enable the data subject to opt out of receiving further messages at little or no cost to the data subject.

Enforcement of the Law

Enforcement of data protection law in the EU is often less visible than it is in the United States. DPA decisions often go unpublished, and the authors of judicial opinions in European legal systems are usually unknown. Moreover, there is no doubt that the broad scope of EU's data protection law and the general lack of resources available to many national DPAs cause many violations to go unpunished.

Nevertheless, the level of enforcement of data protection law is increasing in Europe; criminal penalties, fines, injunctions, and so forth, can be imposed on violators of the law. One German DPA, for instance, required a major company to remove all cookies from its Web site, which significantly affected its online presence. The action was never made public, but the effect was just as serious as if the company had been forced to pay a large fine. A few other prominent examples of enforcement actions include:

- The Italian DPA investigated and prosecuted a company that illegally processed data for commercial solicitation. After discovering the company's failure to register its processing activity, the DPA issued an order blocking further data processing and reported the case to the criminal court.
- The Spanish DPA imposed a fine of several hundred thousand euros against a television producer who failed to appropriately secure a database containing the personal data of participants in a television show and transmitted that data to third-party advertisers without the consent of the participants.
- A Finnish court ordered several top executives of a large telecommunications company to be jailed for illegally monitoring their employees' business telephones. The executives later received suspended sentences.

DPAs initiate most enforcement measures either in response to a complaint from an individual or on their own initiative. Individuals may also bring lawsuits based on data protection violations, but such lawsuits have been rare. Implementation of the General Directive has, however, given individuals an increased opportunity to file lawsuits directly against companies for misuse of personal data, because the directive obligates member states to create a direct cause of action.

Enforcement actions can cover a wide variety of legal violations. Among the most popular grounds for enforcement actions are failing to register data processing with the data protection authorities, sending unsolicited marketing material (particularly spam), and transferring personal data outside the EU without a valid legal basis. In addition, employees and their representatives often file complaints against employers for violations of data protection law.

Emerging Issues: Legislation Dealing with Information Security Breaches

Information security breaches have received the greatest attention from legislators, regulators, and media in the

United States. Commentators in both the United States and the EU have noted the irony that, despite the EU's comprehensive regulation of data protection and the relative lack of such in the United States, the EU has yet to require entities to notify EU residents when their personal data have been exposed as a result of a security breach.

The data protection authorities could, in turn, require security audits, levy fines, and publicize the breach in order to notify affected individuals. Although the proposals would apply only to Internet service providers and network operators, EU courts have previously expanded the reach of the Directive on Privacy and Electronic Communications and could do so again. The requirement to notify data protection authorities, rather than each affected individual, reflects the much lower occurrence of private enforcement (that is, individual lawsuits) in the EU as compared the situation in the United States.

Only a select few breach-related enforcement actions have been reported in the EU, though it is much less common for enforcement actions to be publicized in Europe than is the case in the United States. In December 2006, Vodafone was fined 76 million euros ($103 million) by the Greek DPA, which alleged that Vodafone failed to protect its network from hackers who monitored more than 100 mobile phone accounts. The amount of the fine reflects the high-profile nature of the incident: the hacking occurred during the 2004 Olympic Games in Athens, and the accounts targeted included those of Greek Prime Minister Costas Karamanlis, senior military officers, and journalists. Adding to the scandal, Vodafone's network planning manager in Greece was found dead of hanging not long after he reported to his supervisors that he had discovered the spying software and only one day before the company notified authorities of the hacking. Vodafone is appealing the fine.

Shortly after news of the enforcement action taken on Vodafone, reports surfaced that the Nationwide Building Society was fined £980,000 by the Financial Services Authority (FSA) following the theft in August 2006 of an employee's laptop computer containing customers' personal data. The FSA alleged that Nationwide did not have in place adequate information security procedures and controls. Because Nationwide agreed to settle the action promptly, it received a 30 percent reduction in the original fine of £1.4 million. Nationwide notified its customers of the incident, and both the FSA and Nationwide agreed that the FSA can order regulated financial institutions to provide such notification.

Conclusion

EU data protection law was finalized just before the dawn of the Internet age in the mid-1990s, and this timing is reflected in a number of provisions of the General Directive that are difficult to reconcile with the demands of the online world (for example, choice of law provisions, which are notoriously difficult to apply in an online context). Perhaps most notably, the requirement to legalize personal data transfers to countries that have not received an adequacy determination significantly hinders companies' ability to provide global access to data, contract with data vendors in non-EU jurisdictions, and modify their data flows once they have achieved compliance. This requirement also complicates any number of areas requiring international data transfers, including outsourcing and national security, as evidenced by the disputes between the United States and the EU over transfers of financial information by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and airlines' records of passengers' names.

Achieving compliance with EU data protection law is further complicated by a lack of harmony among the member states that must implement the EU directives. Even some of the most basic concepts of the General Directive (such as the definition of "personal data") differ in each member state's implementation, making it difficult for companies with an extensive presence in the EU to achieve complete compliance with every member state's interpretation of the directive.

There is no doubt that EU data protection law has a substantial impact on day-to-day business practices. Legal obligations—such as providing detailed notices to employees and customers, registering databases with the national data protection authorities, and putting restrictions on international data transfers—impose substantial compliance costs on companies doing business in the EU. Although criticism of the EU approach has intensified because of the increased level of impediments to global data flows, a growing number of jurisdictions, including Russia and Dubai, have adopted comprehensive data protection laws based on the General Directive. Consequently, companies must not only be prepared to navigate the varied data protection compliance issues that arise when doing business in the European Union or with residents of EU member states but also be aware of the privacy and data protection laws that are emerging with increasing frequency across the globe. **TFL**

Elizabeth H. Johnson is an attorney with Hunton & Williams' Privacy and Information Management practice, which was recently named "head and shoulders above the rest" in a Computerworld *survey of corporate privacy officers. Her practice spans all areas of privacy law, including conducting comprehensive privacy and information security assessments, producing records management programs, advising on global data transfer issues, and producing privacy notices, contracts, policies, and procedures. Johnson routinely counsels clients regarding compliance with various statutory and regulatory requirements in jurisdictions such as the EU, federal, and various states including North Carolina, where she is based.*

LABOR *continued from page 15*

caregivers under federal law and should serve as a useful tool for both lawyers and employers alike. **TFL**

Michael Newman is a partner in the Labor and Employment Department of the Cincinnati-based firm, Dinsmore & Shohl LLP, where he serves as chair of the Labor and Employment Appellate Practice Group. He is a vice president of the Sixth Circuit. Shane Crase is an associate in the same department and treasurer of the Cincinnati-Northern Kentucky Chapter. They may be reached at michael.newman@dinslaw.com and shane.crase@dinslaw.com, respectively.

Endnotes

[1]*Enforcement Guidance: Unlawful Disparate Treatment of Workers with Caregiving Responsibilities*, EEOC Notice No. 915.002 (May 23, 2007).

[2]For an insightful treatment of potential causes of action available for family responsibilities discrimination, *see* Joan C. Williams and Consuela A. Pinto, *Family Responsibilities Discrimination: Don't Get Caught Off Guard*, 22 The Labor Lawyer 293 (2007).

[3]*Enforcement Guidance*, *supra* at n. 1 (citing AFL-CIO, Professional Women: Vital Statistics (2006), available at www.pay-equity.org/PDFs, ProfWomen.pdf).

[4]The EEOC notes that in 1975, only 34 percent of mothers with children under the age of 3 worked, compared to 59 percent in 2005. *Id*. (citing Bureau of Labor Statistics, Dep't of Labor, Women in the Labor Force: A Databook 1 (2006), *available at* www.bls.gov/cps/wlf-databook-2006.pdf).

[5]*Id*.

[6]Specifically, the EEOC recognized that "[b]etween 1965 and 2003, the amount of time that men spent on childcare nearly tripled, and men spent more than twice as long performing household chores in 2003 as they did in 1965. Working mothers are also increasingly relying on fathers as primary childcare providers." *Id*. (citing Donna St. George, *Fathers Are No Longer Glued to Their Recliners*, Wash. Post, Mar. 20, 2007, at A2; Suzanne Bianchi et al., Changing Rhythms of American Family Life (2006); Karen L. Brewster and Bryan Giblin, Explaining Trends in Couples' Use of Fathers as Childcare Providers, 1985–2002, at 2–3 (2005), available at www.fsu.edu/~popctr/papers/floridastate/05-151paper.pdf).

[7]538 U.S. 721, 728 (2003).

[8]*Id*. at 729 (quoting 29 U.S.C. § 2601(b)(4) and (b)). The court outlined the significance of such gender-based discrimination: "Congress determined [that] '[h]istorically, denial or curtailment of women's employment opportunities has been traceable directly to the pervasive presumption that women are mothers first, and workers second. This prevailing ideology about women's roles has in turn justified discrimination against women when they are mothers or mothers-to-be.'" *Id*. at 736 (citation omitted).

[9]365 F.3d 107, 113, 124 (2nd Cir. 2004).

[10]*Id*. at 121. *See also Ramos v. Centennial P.R. Wireless Corp.*, 217 F.3d 46, 55-56 (1st Cir. 2000) (finding that the jury could find a pretext where the plaintiff's supervisor questioned the plaintiff on "her ability to balance her current work and parental responsibilities," along with several other comments, and terminated plaintiff two weeks later).

[11]383 F.3d 580, 582–583 (7th Cir. 2004).

[12]478 F.3d 640, 649 (4th Cir. March 5, 2007).

[13]332 F.3d 1150, 1154 (8th Cir. 2003).

[14]In its guidelines, the EEOC noted that "[t]here is substantial evidence that workplace flexibility enhances employee satisfaction and job performance. Thus employers can benefit by adopting such flexible workplace policies by, for example, saving millions of dollars in retention costs." *Enforcement Guidance*, supra at n. 1 (citing Corporate Voices for Working Families, Business Impacts of Flexibility: An Imperative for Expansion 13 (2005), available at www.cvworkingfamilies.org/flex_report.shtml; Families and Work Institute, National Study of Employers 26 (2005), available at familiesandwrk.org/eproducts/2005nse.pdf.

Judicial Profile Writers Wanted

The Federal Lawyer is looking to recruit current law clerks, former law clerks, and other attorneys who would be interested in writing a Judicial Profile of a federal judicial officer in your jurisdiction. A Judicial Profile is approximately 1,500–2,000 words and is usually accompanied by a formal portrait and, when available, personal photographs of the judge. Judicial Profiles do not follow a standard formula, but each profile usually addresses personal topics such as the judge's reasons for becoming a lawyer, his/her commitment to justice, how he/she has mentored lawyers and law clerks, etc. If you are interested in writing a Judicial Profile, we would like to hear from you. Please send an e-mail to Stacy King, managing editor, sking@fedbar.org.

Q: Can anything be done about preserving the distinction between *who* and *whom*? Or is the difference worth preserving when almost everyone ignores it?

A: Sadly—in my view—the question about whether the distinction between *who* and *whom* is worth saving is academic. Almost inevitably *whom* will disappear. Even writers you would expect to preserve the distinction do not. Item: In her weekly column in *Newsweek*, Janet Bryant Quinn asked, "Now *who* do you trust?" Item: A *New York Times* reporter wrote, "President Bush advocated scholarships for Cubans, *whom* he said should be able to vote." (Emphasis mine.) Both *who* and *whom* in those sentences are ungrammatical.

Some readers of this column are unhappy at the loss of the distinction between *who* (the subjective form of the relative pronoun) and *whom* (the objective form). One reader who would like to have *who* and *whom* used properly wrote that he had asked an English teacher how she teaches her students the difference between the two. Her response was, "No one bothers about that any more. We just let the students use *who* for everything." (If she is younger than 40, she probably doesn't know the difference herself.)

Even conservative grammarians have given up on whom. Ernest Burchfield, in his new *Fowler's Modern English* (1996) wrote that "*whom* is moribund or at best socially divisive" and "to whom do you wish to speak?" is "frozen, archaic, stifling or artificial."

That opinion does not seem justified. I agree that most people would say, "Who do you wish to speak to?" But when they write, they would not write, "To who do you wish to speak?" They would instead use the objective form *whom*: "To whom do you wish to speak?" Burchfield's biting criticism of *whom* as "frozen, archaic, stifling or artificial" should be directed at the syntax of the sentence, not the pronoun. However, there is no question that *whom* is on its way out. The majority has so decided.

Young people, especially, enjoy changing the meaning of words. For example, our granddaughter, a new teacher, told us that some of her students were "needy." To our generation, that adjective describes a person who needs financial help. My granddaughter's generation has expanded the meaning of *needy*, so that it now includes wealthy young people who lack self-esteem. And only yesterday, it seems, the coinage *nerd* described a bookish, serious student. The noun *nerd* had replaced another innovation, *grind*. But I am told that *nerd* is also out-of-date. A serious student is now a *swot* or a *wonk*.

And the coinage *wonk* has already spawned an adjective form. To emphasize the importance of her committee, a member of the Senate Governmental Affairs Committee said, "This [committee] may seem a wonky assignment, not as sexy as, say, the Armed Services Committee." In that one comment, she changed the meaning of both adjectives. The adjective *wonky* seems to mean "dull"; the adjective *sexy* is dehumanized and seems to mean "glamorous."

This brings to mind Humpty Dumpty's response to Alice, who had complained that, although he used *glory* to mean "a nice knock-down argument," it didn't really mean that:

> "When I use a word," Humpty Dumpty said, in a rather scornful tone, "it means just what I choose it to mean, neither more nor less."
>
> "The question is," said Alice, "whether you *can* make words mean so many different things."
>
> "The question is," said Humpty Dumpty, "which is to be master—that's all."

Every newborn human takes part in language change. But along with all those who change the meaning of words that are already part of the language or abandon old words while introducing new words, there must be other speakers applying a brake on change. Without that restraint, change would occur helter-skelter. If words changed their meanings at the whim of every speaker, our "common" language would no longer communicate. Oliver Wendell Holmes said, "We ask, not what *this* man meant, but what those same words would mean in the mouth of any normal speaker of English, using them in the circumstances in which they were used" (taken from Martin Mayer, *The Lawyers*, 1967).

Life in Humpty Dumpty's world would be confusing. But a language that never changed would be no more normal than one of untrammeled change. Language should and inevitably will change when a large majority of its speakers agree that it should. That is why the rule governing the use of *who* versus *whom* is no longer enforceable and therefore no longer valid.

An anecdote told by Justice Robert H. Jackson supports this proposition. As a young lawyer, to validate his argument before an upstate New York judge, Jackson cited a case that had been newly decided by the Supreme Court, and he handed the presiding judge the advance sheets to prove his point. The judge handed them back, glared, and said, "I don't take no law from no magazines." Like that judge, we English speakers "don't take no law from no magazines." **TFL**

Gertrude Block, lecturer emerita at the University of Florida College of Law, is author of Legal Writing Advice: Questions and Answers *(William S. Hein Co.) and* Effective Legal Writing *(5th edition, Foundation Press, 1992). She can be reached at block@law.ufl.edu or by snail-mail: Gertrude Block, Lecturer Emerita, Emerson Hall, University of Florida, Gainesville, FL 32611.*

Living Speech: Resisting the Empire of Force

By James Boyd White

Princeton University Press, Princeton, NJ, 2006. 236 pages, $29.95.

REVIEWED BY THOMAS HOLBROOK

This is a book about disrespect—and about the benefits of practicing it. Disrespect is particularly vital to practitioners of law, James Boyd White tells us, as well as to others who wish to be truly human and to overcome the fatuities of power and the coils of the powerful. So important stuff here, if we choose to heed it.

Where does this power reside, and how are we to resist it? White's answer is surely applicable to the political circumstances in our time, because, as he explains, the force that coerces improper actions isn't physical, but almost always mental: "it really lives, in the mind [not the barrel of a gun]; without that life it would have no force at all." The danger comes not from the physical coercion of George Orwell's *Nineteen Eighty-Four*, but from the self-imposed linguistic bondage of Joseph Heller's *Catch-22*.

As a professor of law and of Eng-lish at the University of Michigan, White is ideally suited to examine the bondage that language can exact from those it overmasters. The remedy is to master the language, as he has argued in prior books, *The Legal Imagination* and *The Edge of Meaning* among them.

White's proof text for the argument of *Living Speech* is from Simone Weil, and is translated as "No one can love and be just who does not understand the empire of force and know how not to respect it," although "know how to disrespect it" might be a less awkward Englishing.

What does this mean? What does mere language have to do with the starwarian "empire of force"? How does "living speech" matter to us, on our quotidian plane of prosaic reality? Why should we care?

It is because "prosaic" is the prime deceptor, White argues, "and much is at stake." For we can live on one plane, that of "the reiteration of clichés, formulas, slogans—dead language really," where we can try "to sound like a lawyer, not to be one," become mentally and morally dead, in White's conception. Or we can attain utterance of a second kind:

> speech that comes from the center of the person, and is addressed to the center of its audience . . . speech upon which both individual and shared life can be built. ... For it is only this ... living speech, that ... makes possible the real—if always imperfect—communication of mind with mind. ... Indeed it is what enables any of us to be a person in the first place.

Thus, "living speech" is the method we are to use to resist, then to overcome, Weil's "empire of force" that White adopts as his metaphor for the spiritual and ethical death that abidingly prevails in so much of contemporary life—the death conveyed by "clichés and received ideas and formulas and slogans presented as though they could carry the work of thought and writing":

> [T]he strong forces of advertising and propaganda [that] constantly work to trivialize our language and experience, to infantilize us as political actors and thinkers, and to reduce us to consumers and voters with defective minds. How to resist these forces, ultimately forces of death ... is ... both the central question of individual life and the largest cultural and political issue of our era.

The "empire of force" uses this murky and formulaic "second kind" of language (cliché, formula, slogan, received opinion) to deceive and enslave us, as George Orwell pointed out long ago in his essay "Politics and the English Language." Orwell focused primarily on the political uses of deceitful language, whereas White explains that, by succumbing to such language we not only are manipulated politically but also actually lose our human value. We cease to "be" in any clear, active, and humane sense and become more like echoes than persons. "Living speech," in short, can be uttered only by people who are "present as a mind, a person" in their speech and writing.

What does mere language have to do with the starwarian "empire of force"? How does "living speech" matter to us, on our quotidian plane of prosaic reality? Why should we care?

White anatomizes this "being present" by analyzing several legal opinions and literary works (and one that, at heart, is both). He opens with Homer and Dante, then proceeds through Frost, Shakespeare, William Carlos Williams, and Plato's *Phaedrus*, alternating with legal opinions that are various and extensive, "alive" and "dead," with several from the U.S. Supreme Court. And there is a brief letter by Lincoln.

A high point of the book is White's equation of the U.S. Supreme Court with Athenian tragic drama. The Court, he explains, "exists primarily in cultural and imaginative and political space." Just so classical Athenian drama. Further, "it is a public arena ... one function of which is to bring certain stories and the problems they present into public attention ... for education or enlightenment." In a footnote to this remark, White explains how immensely important the juridical *opinion* is to this process and how clear, explicating prose is absolutely necessary for living law—law that is "present as a mind, a person": "Imagine ... that the Court had been forbidden to write opinions and that its judgments had to stand on their

REVIEWS *continued on page 52*

own, undefined and uninterpreted. This would destroy the possibility of law as we know it." One can scarcely imagine that, in a free and open society.

White's excerpting of Court opinions to illustrate "dead" and "living" expression is too extensive to quote illustratively here, but a brief negative example from a Court opinion may suffice:

> The statute proscribes the visual depiction of an idea—that of teenagers engaging in sexual activity—that is a fact of modern society and has been a theme of art and literature throughout the ages. ... It is, of course, undeniable that some youths engage in sexual activity before the legal age, either on their own inclination or because they are the victims of sexual abuse.

Ashcroft v. Free Speech Coalition, 535 U.S. 234, 246, 247 (2002).

This is a meaningless bladder of blah blah blah, as White points out: "[I]n this part of its opinion and indeed throughout [the Court] engages in analysis at the level of ... formula or cliché. It is the stuff of law school outlines, not a distinguished judicial opinion. What I miss ... is the presence of a mind actually engaged with a difficult problem of understanding and judgment."

In all this we may think that White disrespects too avidly, that he makes impossible demands on legal and other writers, given the pace and pressure of modern life. If so, we need only to look at the letter by Lincoln that he includes as the "living" expression we must aspire to, written under as much pressure as any writer has ever had to bear. Lincoln writes to Gen. Joseph Hooker in January 1863:

> I have placed you at the head of the Army of the Potomac. Of course I have done this upon what appear to me to be sufficient reasons. And yet I think it best for you to know that there are some things in regard to which, I am not quite satisfied with you. I believe you to be a brave and skil[l]ful soldier, which, of course, I like. I also believe you do not mix politics with your profession, in which you are right. You have a confidence in yourself, which is a valuable, if not an indispensable quality. You are ambitious, which, within reasonable bounds, does good rather than harm. But I think that during Gen. Burnside's command of the Army, you have taken counsel of your ambition, and thwarted him as much as you could, in which you did a great wrong to the country, and to a most meritorious and honorable brother officer. I have heard, in such a way as to believe it, of your recently saying that both the Army and the Government needed a Dictator. Of course it was not *for* this, but in spite of it, that I have given you the command. Only those generals who gain successes, can set up dictators. What I now ask of you is military success, and I will risk the dictatorship. The government will support you to the utmost of its ability, which is neither more nor less than it has done and will do for all commanders. I much fear that the spirit which you have aided to infuse into the Army, of criticizing their Commander, and withholding confidence from him, will now turn upon you. I shall assist you as far as I can, to put it down. Neither you, nor Napoleon, if he were alive again, could get any good out of an army while such a spirit prevails in it.
>
> And now, beware of rashness. Beware of rashness, but with energy, and sleepless vigilance, go forward, and give us victories.
>
> *Yours very truly*
> *A. Lincoln*

This is writing that disrespects the empire of force as strongly as can be imagined. Lincoln's prose is clear, plain, direct, empathetic but forceful, legalistic but nonlegal. We are so unaccustomed to such writing that it shocks us with its directness (which is, after all, just truth), but when we try to change it, or excerpt it, we find that it cannot be modified or abbreviated without serious loss. It is written by the whole person, the whole mind, and it fully engages the mind of the recipient (one cannot imagine Hooker's ever forgetting this letter). We could scarcely conceive of a fitter example of what White calls for in this book:

> It is possible for writing in the law, as in other fields, to call the reader into life, life with language and life with other people, and hence into a world in which love and justice are possibilities. It can resist the forces of death and empire—of advertising and propaganda, of cliché and commodification—by insisting upon a kind of speech that speaks from person to person, mind to mind, and recognizes that in all our language uses we are claiming meaning for the experience of ourselves, and others, meaning for which we are responsible.

This is a compelling book—an appropriate tract for our times that deserves widespread and careful reading in an era deeply infected by the linguistic plagues White disinfects through disrespect. However, because most of the material is reworked from earlier talks and essays, perhaps the best way to read this book is one chapter at a time, with lapses and considerable cogitation between. **TFL**

Thomas Holbrook has been a student, writer, editor, and teacher most of his adult life. He is retired from the Library of Congress' Congressional Research Service.

Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims

By Judith M. Collins

John Wiley & Sons, Inc., Hoboken, NJ, 2006. 252 pages, $39.95.

Reviewed by Arthur L. Rizer III

Are you concerned about identity theft? A better question, according to Judith M Collins, the author of *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims*, is: What are you going to do if you are a victim of or investigating a case of identity theft?

Collins, a highly regarded expert on crimes involving identity theft and a former professor at the School of Criminal Justice at Michigan State University, notes that, despite the widespread attention that these crimes command, they continue to increase in severity and frequency. Even more disturbing is that victims and law enforcement officers appear to be ill-equipped and insufficiently educated to prevent and combat these crimes. Whereas in the pre-Internet era, you could prevent most theft merely by locking your doors, today you must take steps that include shredding your garbage, installing firewalls on computers, and reducing your electronic profile. As for the police, whereas in the past they might have achieved results merely by chasing down leads, today they are faced with tracing international e-mails and digging through IP addresses and URLs across the World Wide Web.

Collins follows a five-step format in investigating these types of crimes:

1. Know the crime and understand the criminal.
2. Equip computer security for identity theft investigations.
3. Configure the computer for online investigations.
4. Understand the victim, then prepare to launch the investigation.
5. Authenticate the facts of the case (in particular what the victim reported) and investigate the crime itself.

The chapters in the book follow this basic format, with the first half of the book providing background on the problem of identity theft crimes by giving examples of real cases—both solved and unsolved—and the second half of the book moving from explaining crimes of identity theft from a technical or victims' perspective to investigating the crimes.

This book is unique in the extent of detail it provides for actually conducting an investigation. The real gem in the book, however, is the practical exercises it provides to enable the reader to actually try to do what is being taught. One learns not merely the concepts involved in investigating identity theft; one learns how to investigate it.

Investigating Identity Theft contains a bounty of useful information. You will learn how to put your name on the Do Not Call list, how to write a letter to a business explaining that you were a victim of identity theft (yes, sample letters are provided), and how to find the code in an e-mail so that you can decipher where it really came from. Almost more useful is the 165-page appendix that contains a list of hundreds of useful Web sites that allow the user to find anything from zip codes to registered truck drivers in Alabama. This is all presented in an easy-to-read format with concise statements of themes complemented by dozens of graphs for some of the more complex discussions and scenarios.

Although *Investigating Identity Theft* would be helpful to an official investigator, the book would be especially useful to a victim of identity theft who seeks to get his or her life back together and track down the perpetrator—although Collins states explicitly that victim investigators should not try to confront suspects; rather, they should gather information on the computer and turn it over to law enforcement officials. This is also a good idea because, as Collins observes, police spend most of their time investigating conventional violent crimes such as rape and murder. Therefore, Collins notes that, by being your own investigator, you not only can help the police with their legwork but also may cure yourself of the feeling of being a victim. In the past, Collins writes, "the most a victim could do was prevent further abuse and accept the fact that the perpetrators may never be caught and convicted." This is no longer the case—thanks, in part, to this book.

Investigating Identity Theft does have a few shortcomings. In particular, because it is filled with useful information, a heartier index would make future research more convenient. My only other criticism—which is not really a criticism, because the problem is inherent in the subject matter—is that the book runs the risk of being outdated very soon. This is particularly true of the technical data contained in the graphs and practical exercises. Indeed, while conducting some of the practice exercises, I noticed that some of the Web sites had already changed, making those exercises obsolete. Nevertheless, *Investigating Identity Theft* will be useful to victims of identity theft, law enforcement officers, and anyone who wants to prevent identify theft. **TFL**

Arthur Rizer is an attorney with the U.S. Department of Justice. The views expressed in this review do not necessarily represent the views of the Department of Justice.

Liberty Under Attack: Reclaiming Our Freedoms in an Age of Terror

Edited by Richard C. Leone and Greg Anrig Jr.

Public Affairs, New York, NY, 2007. 275 pages, $15.95.

Reviewed by Kevin J. Barry

It has been said that what happens to a person is often less important than how that person responds to what happens. That principle underlies the essays in this remarkable and timely book. The attacks of Sept. 11, 2001, brought forth a new era in America—an era defined not so much by the attacks themselves as by the choices our government made as to how to respond to those attacks. Now, more than five years later, the implications of those choices are becoming more and more clear. *Liberty Under Attack* is a compilation of essays that presents the views of 12 respected experts, each assessing an aspect of our government's response to Sept. 11. The compelling message of the book is that anyone who cherishes the freedoms that have been part of America's ideals since the founding of our nation should now be apprehensive—if not distinctly alarmed.

The editors open with an introduc-

REVIEWS *continued on page 54*

tion that summarizes the situation after five years of fighting the "global war on terror" and introduces the essays that follow. Next are five essays under the heading "Discarding Democracy." Alan Brinkley leads off by pointing out that, historically, during times of crisis, security always takes precedence over civil liberties, but that it is a myth that civil liberties always snap back after the crisis has ended. In any case, because the current crisis has no clear end, we should be especially vigilant when it comes to preserving our civil liberties. David Cole follows with an analysis of the extreme viewpoints of executive power promulgated by John Yoo and illustrates how these views were exactly what President George W. Bush wanted to hear. Gary Hart indicts Congress for its abject failure during the first five years of the Bush presidency to fulfill its constitutional duty to act as a check on executive power, and he complains that both the Republicans, when they held a majority in Congress, and too often many Democrats, behave as if their oath had been to support and defend not the Constitution, but the President. John Podesta writes about the administration's push to reclassify historical documents in order to take them out of the public view and the White House's penchant to classify material and keep secrets not for national security reasons but to avoid embarrassment. Podesta argues that the result has been far less security, because fewer secrets and a better informed public are the route to enhanced national security. Peter Osnos then outlines the tension that has existed between the media and various administrations, and the Bush administration's particularly effective efforts to limit not only adverse publicity but also even the reporting of facts needed for the Congress and the public to be able to evaluate the administration's pronouncements—pronouncements that are too often at odds with the truth.

Three essays appear in the second section of the book, "Americans Under Watch." Stephen J. Schulhofer leads with a discussion of the PATRIOT Act, which he sees as emblematic of the "surveillance society." He argues that the PATRIOT Act, whose provisions have "alarming implications," was reauthorized in March 2006, despite the administration's having provided "almost none of the concrete details necessary to assess the provisions or to understand their impact." Schulhofer reviews many of the act's most troublesome provisions and discusses the administration's defiance of the law in its use of warrantless electronic surveillance. Next, Patrick Radden Keefe, in "The Espionage Industrial Complex," argues that the current situation—with technically deficient government intelligence services relying on private-sector expertise—manifests the "grave implications" that President Eisenhower saw in the "conjunction of an immense military establishment and a large arms industry." Keefe fears the real possibility that "by incrementally diminishing our expectations of privacy and liberty in exchange for a promise of elevated security that ultimately proves illusory, we will end up both unsafe and unfree." Finally, Aziz Huq, in "The New Counterterrorism: Investigating Terror, Investigating Muslims," addresses the targeting of Muslims via new investigative techniques and the use of "preventive" prosecutions. He demonstrates that such efforts have been ineffective in finding terrorists but have had a huge cost in the loss of trust within Muslim communities and the consequent loss of tips from individuals in these communities.

In the final section of the book, "Is This Justice?" Stacy Sullivan leads off by addressing the egregious situation in Guantánamo from a variety of perspectives, including the departure from American principles, such as the presumption of innocence, the right to counsel, and the right not to be incarcerated indefinitely without charge or trial. Joseph Lelyveld expands on the issue of the detainees, analyzing the effect of our abandonment of the Geneva Conventions and the impact of domestic law such as the Detainee Treatment Act and comparing British measures used in dealing with terrorist suspects during the same period. Ann Beeson assesses the Bush administration's use of secrecy in investigations (for example, national security letters and secret warrantless wiretaps) and litigation (state secrets privilege) as well as governmental abuses in both. Finally, Eugene R. Fidell closes this extraordinary collection with "Disorder in Military Courts," in which he analyzes problems related to courts-martial of American forces for a variety of crimes as well as the huge legal problems and perception issues raised by the use of military commissions to try non-citizen enemy combatants.

It was Benjamin Franklin who cautioned that those who would "give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." In this marvelous compilation, the authors present compelling evidence and arguments that, in its response to the attacks of Sept. 11, the executive branch of our government has ignored domestic and international law; created new legal systems; defined new categories of persons neither civilian nor military; used abusive interrogation tactics amounting to torture against such persons; spied on its own citizens; and used fear, secrecy, and intimidation as weapons in support of its preference for security over liberty—all to the detriment of traditional American principles and values. Moreover, the authors show that the legislative branch has been complicit in these wrongs by its utter failure to fulfill its constitutional duty to oversee the executive branch and to serve as a check on its abuse of power. *Liberty Under Attack* should be mandatory reading for every member of Congress, every federal judge, and every employee of the executive branch. It should be read, in fact, by everyone who cherishes American freedoms or fears unchecked governmental power. **TFL**

Capt. Kevin J. Barry, USCG (Ret.) is a director of the National Institute of Military Justice and past president of the Pentagon Chapter.

Reflections on Freedom of Speech and the First Amendment

By George Anastaplo

University Press of Kentucky, Lexington, KY, 2007. 336 pages, $70.00 (cloth), $26.95 (paper).

Reviewed by Joseph Goodman

Reflections on Freedom of Speech and the First Amendment is a companion to George Anastaplo's prior book, *Reflections on Constitutional Law* (which I reviewed in the May 2007 issue of *The Federal Lawyer*). The new book builds toward a greater understanding of both the historical basis and boundaries of freedom of speech and the importance of freedom of speech for responsible and effective republican government. The first part of the book examines the background and principles of free speech and includes brief chapters on Plato, St. Paul, Thomas More, John Milton, and Patrick Henry, as well as on some of this nation's founding documents. The second part of the book examines leading Supreme Court free speech cases and includes essays on Justice Hugo Black and Winston Churchill.

Anastaplo's passion for the subject of freedom of speech can be traced back to 1954, when he was denied admission to the Illinois bar for refusing, on First Amendment grounds, to answer questions about his political beliefs. Anastaplo argued his case all the way to the U.S. Supreme Court, which, in *In re Anastaplo*, 366 U.S. 82 (1961), ruled against him by a 5 to 4 majority, even though there was no evidence that he was a Communist or any other kind of threat to the republic. The Court concluded that Anastaplo "holds the key to admission in his own hands," while dissenting Justice Hugo Black defended without qualification Anastaplo's First Amendment right to silence, writing, "We must not be afraid to be free."

It is not surprising, then, that Anastaplo argues throughout the book that "responsible and effective self-government" depends on a "wide-ranging, if not even absolute," protection of political discourse. He begins with Plato's *Apology of Socrates*, "one of the sacred texts upon which Western Civilization rests." He argues that "the inspiration offered by the *Apology* can usefully be considered vital to the most serious purposes of the First Amendment. The claims of what *we* call 'conscience' are elevated. And citizens can be encouraged thereby to speak out about the issues of concern to the community." Anastaplo also finds the career of St. Paul a source for modern freedom of speech. In affirming one's faith, frankness of speech is necessary, "even to the extent of openly calling into question the deeds and the doctrines of those in authority."

"A 1521 petition to King Henry VIII, by Sir Thomas More as Speaker of the House of Commons," Anastaplo writes, "is said to be the earliest document in which parliamentary freedom of speech is recognized." More than a century later, in 1644, John Milton produced the celebrated *Areopagitica*, which is a pamphlet that argues against "any *system* which subjects writings to official scrutiny before publication." Anastaplo describes *Areopagitica* as "serving as the 'cornerstone' upon which freedom of speech can rest." He then discusses the career of Patrick Henry, whose resolutions "became the basis for violent agitation [against the British] from Boston to Charleston." Emphasizing that freedom of speech in the United States was established before the Bill of Rights, Anastaplo points out that Patrick Henry's famous exclamation, "'[G]ive me liberty, or give me death!' ... is one of the most memorable exercises of freedom of speech in American history, an exercise that did not depend for its legitimacy or effectiveness on the First Amendment."

With respect to the First Amendment, Anastaplo views the freedom of speech clause as primarily intended to protect political speech. He discusses the Sedition Act of 1798, which was a "consequence of the fear in this Country, especially among the Federalists, of French meddling in American affairs" and "was considered oppressive by people accustomed (from even before Independence) to American-style liberty." The Sedition Act turned out to be "the beginning of the permanent decline of the Federalist Party in this Country."

Following a chapter on John Stuart Mill's *On Liberty* (1859), which "is so celebrated that it can be identified in our own time ... as virtually an appendix to the Declaration of Independence and the Constitution of the United States," Anastaplo examines freedom of speech and the approach of the Civil War. After discussing the South Carolina Declaration of the Causes of Succession, he draws attention to the relation between free speech and responsible self-government: "The intimate relation between freedom of speech and the necessary political processes of the Country was again and again evident even during that soul-wrenching period of genuine 'clear and present danger' for the United States."

The second part of *Reflections on Freedom of Speech and the First Amendment* begins with an essay on "The Naive Folly of Realists: A Defense of Justice Black (1937–1971)," in which Anastaplo responds to another scholar's assessment of Justice Black "as a constitutional fundamentalist." Oddly, Anastaplo does not reveal the name of the scholar or identify the work to which he is responding, even though his primary purpose in this essay is to rebut the scholar's "question[ing] whether there is any 'original understanding of the Constitution' by which judges, or anyone else in authority, can and should take their bearings." Anastaplo argues that Justice Black's career was "very much grounded in the constitutional principles and expectations of the American regime."

Anastaplo then criticizes a few Supreme Court decisions that restricted political speech, starting with *Schenck v. United States* (1919), which includes two of Justice Holmes' most famous phrases: speech may be punished only when it creates a "clear and present danger," but freedom of speech "would not protect a man in falsely shouting fire in a theater and causing a panic." In *Schenck*, the Court affirmed the convictions of defendants who had circulated to military draftees leaflets "calculated to cause insubordination and obstruction." Anastaplo argues that *Schenck* "set an unfortunate precedent in First Amendment law," and that, in fact, "the language used by Justice Holmes can be understood to have done far more to weaken the security of the United States than anything that the Schenck defendants and their successors in the docket ever tried to do."

Anastaplo also discusses *Debs v. United States* (1919), which was de-

REVIEWS *continued on page 56*

cided one week after *Schenck* and affirmed the conviction of Eugene V. Debs pursuant to the Espionage Act of 1917 for speaking out against the recruitment of soldiers during World War I. Anastaplo believes that *Debs* "may be the most disgraceful prosecution for unpopular political speech in the history of the Country," and that "the Supreme Court, in the principal sedition cases in the twentieth century, tended to reassure ... those among us who have been determined to suppress any sedition that they have come to believe a threat to the Country."

Discussing Justice William O. Douglas' concurring opinion in *Brandenburg v. Ohio* (1969), Anastaplo points out that Justice Douglas recognized the Cold War "as having helped weaken the Speech and Press guarantees recognized by the First Amendment." Anastaplo also makes the interesting assertion that "the Cold War may have contributed to the determination of the Government of the United States, including its Courts, to favor racial desegregation in the interest of an effective American foreign policy." As he does often in this book, however, he makes this isolated comment without further discussion or citation, leaving the reader to do research on his own. (That is easy enough in this case; see, for example, Michael L. Krenn, ed., *Race and U.S. Foreign Policy During the Cold War*, published in 1998.)

Anastaplo writes:

> [F]reedom of speech and of the press, as protected by the First Amendment, is designed primarily for the benefit of the community as a whole, *not* primarily for the benefit of those who may want to say something. It should be obvious that when critical opinions are suppressed, the community is deprived of something that it may very much need to hear. And such opinions are apt to be suppressed if those holding them are routinely subjected to prosecution because of associations intimately linked to those opinions.

In light of this view, Anastaplo does not believe that nonpolitical speech deserves the same protection as political speech. Anastaplo criticizes *Cohen v. California* (1971), in which the Supreme Court overturned the conviction of a young man who, in a municipal courthouse, had worn a jacket that said "Fuck the Draft." Anastaplo sees *Cohen* as incorrectly placing "the emphasis upon an individual's desire to exhibit 'the depth of his feelings' about whatever might move him. It is *not* to recognize what the community is accustomed and entitled to expect from those who, sometimes at great personal risk, challenge the wrongheaded policies of the day." As to the Court's suggestion that "[t]hose in the Los Angeles courthouse could effectively avoid further bombardment of their sensibilities simply by averting their eyes," Anastaplo comments, "This means, in effect, that an aggressive young man gets in one slap at every unsuspecting bystander he chances to encounter as he walks through a public place. *He*, it seems, should not be obliged to control *him*self at all, but only those he indiscriminately attacks."

It is not surprising that Anastaplo is also not sympathetic to free speech protection for obscenity, believing that "[a]n unregulated freedom of expression can, in some circumstances, undermine the character and education needed for sustained self-government." He adds: "Even more insidious may be the spiritual waste we are generating by developing, and thereafter by catering to, all kinds of lascivious tastes. Technological developments have been such that it will soon be, if it is not already, impossible for any sizable community to exercise effective control over the corrupting influences to which its members are apt to be exposed. It can then become largely a matter of chance who does what to whom."

Anastaplo is also highly critical of the Universal Declaration of Human Rights, which the United Nations adopted in 1948. Although the document promotes "a democratic society" as the only legitimate form of government, Anastaplo conjectures that "[i]t is unlikely that even half of the countries represented in the United Nations General Assembly which promulgated this Declaration were 'democratic' in the sense indicated therein." He also notes that the declaration insists upon the rule of law, including entitlement to a proper trial when detained, "[b]ut is evident throughout the Declaration that the countries subscribing to it do not have 'in their bones' any 'feel' for the power of the writ of *habeas corpus* in the hands of a substantially independent judiciary." He compares the document to the Soviet Constitution: "The limited effectiveness of noble proclamations, when not grounded in a people's character and experience, was evident in the noble rhetoric of the Soviet Constitution. The wide-ranging rights guaranteed there, imported for the most part from the West, were mocked by the routine political and legal oppressiveness of the Soviet regime. The dependence of the development of truly free, or at least decent, institutions does depend considerably upon the circumstances of a people."

Entitled "The Future of the First Amendment?," Anastaplo's final chapter is philosophical. He returns to his theme of the effect of technological development on society and expresses concern about the impact of the Internet on the community and the character of the people. "[P]olitical tyranny *is* apt to be undermined, or at least threatened, by the Internet and its successors. But also apt to be undermined are the sense of community and the character of the people. This can amount to another, even more insidious, form of tyranny. ... Rampant individualism is promoted even as one is more and more entangled. The unprecedented anonymity now available in what one says publicly can permit one to be irresponsible. At the same time, one can become, as the target of the irresponsible utterances of others, ever more vulnerable."

Reflections on Freedom of Speech and the First Amendment reflects more than half a century of contemplation of freedom of speech issues by Anastaplo since his 1954 Illinois bar controversy. It is well worth reading. **TFL**

Joseph Goodman is a law clerk for Hon. David Thompson of the U.S. Court of Appeals for the Ninth Circuit. He is also an adjunct professor at Thomas Jefferson School of Law.

Finn: A Novel

By Jon Clinch

Random House, New York, NY, 2007.
287 pages, $23.95.

Reviewed by Henry S. Cohn

Jon Clinch's *Finn* is certainly evidence of the truth of Ernest Hemingway's bon mot that "[a]ll modern American literature comes from one book by Mark Twain called *Huckleberry Finn*." Clinch, who formerly had a career in advertising, has written his first novel—a fictional biography of pap Finn, Huck's father. Although the premise is innovative, the work moves uncomfortably away from both the facts and the flavor of the Twain classic.

In Twain's *Adventures of Huckleberry Finn*, pap appears suddenly and asserts his right to Huck's assets. Twain brilliantly portrays the resulting proceedings in a 19th-century juvenile court, and his description of pap's claimed rehabilitation from alcoholism still strikes a chord in readers today. Later, Twain movingly pictures pap's delirium tremens and Huck's escape from his father's control. Then, just as Huck and the slave Jim begin their raft adventures, they find a frame house floating down the Mississippi.

This house is a treasure trove for them, and they take away most of its contents. One of the highlights of Twain's novel is his description of the inside of the house. "There was heaps of old greasy cards scattered around over the floor, and old whisky bottles, and a couple of masks made out of black cloth; and all over the walls was the ignorantest kind of words and pictures, made with charcoal." Men's and women's clothing were "hanging against the wall. ... And there was a bottle that had had milk in it; and it had a rag stopper for a baby to suck. We would a took the bottle; but it was broke." Jim also finds a dead man on the premises. You can guess who it is.

Aspects of *Huckleberry Finn*—especially Twain's description of the house—become the raw material for Clinch's story. In Clinch's novel, pap is the younger son of a prominent racist Illinois judge. While pap has become a derelict, the judge's other son has become an attorney and a slavish follower of his father. Clinch also makes use of Twain scholar Shelley Fisher Fishkin's thesis that Huck's mother was black. Pap cohabits with a black woman, Mary, with whom he has a love-hate bond. Needless to say, this interracial relationship completely alienates pap's father from pap. Although Clinch leaves the relationship ambiguous, Mary seems to be Huck's mother. Pap, who has a violent temper, eventually commits an assault in a tavern and receives a prison sentence. On pap's release from prison, he abuses Mary, who escapes with Huck across the Mississippi to St. Petersburg, where the Widow Douglas lives. Clinch finishes his tale by relating pap's last days in the aforementioned frame house.

Clinch's dialogues are well-written, and he builds up tension effectively. Unfortunately, however, he adopts the modernistic technique of not giving his tale a beginning, a middle, or an end. The story jumps back and forth among various events in pap's life, and it is difficult at times to reconcile Clinch's version of events with Twain's version. For example, in *Huckleberry Finn*, Huck escapes from pap, spends a few days with Jim, and then discovers the frame house. *Finn*, however, implies that Huck had escaped much earlier.

Clinch's pap engages in domestic violence, substance abuse, and racism, and he is too one-dimensional—unmitigated evil. Twain's novel, by contrast, is much more nuanced. He populated his novel with frauds and hypocrites, such as the duke and the king, and, in the misdirected wealth of the Shepherdson and Grangerford households, he showed the excesses of capitalism. In Twain's portrayal, characters like pap are incompetent and angry, but they usually do not do serious harm to others. Nevertheless, pap and the unfortunate Boggs were tragically doomed to death by their alcoholism. Twain, unlike Clinch, shows Huck's struggles with his own racist attitudes. Twain's multidimensional characters are more believable because they are more real.

Twain's tone is also different than Clinch's. Drafts of *Huckleberry Finn*, some of which became available only in the last few years, reveal that Twain's initial description of the frame house was more graphic than the one that appears in the final version. In a 1996 edition of *Huckleberry Finn*, Professor Victor Doyno notes that the house scene originally had a "nightmarish quality" but that Twain revised it to make the depiction less disturbing. Clinch's novel intends to shake up the reader by painting a picture of a reprehensible life. Twain's approach is more effective and is infinitely more enjoyable. **TFL**

Henry S. Cohn is a judge of the Connecticut Superior Court.

Foundation Contributors—June
Ludwig J. Abruzzo
Brian M. Ballay
Elizabeth Bazan
Bryan H. Beauman
Jeffrey E. Blivaiss
Gregory D. Boos
Adam LH Bramwell
Rex Lamont Butler
George B. Butts
Joseph F. Cimini
Charles D. Cole
Kathryn Collard
Ashley R. Cook
Adriana Cortina Martinez
Lisa Counters
John P. Coyle
Paul G. Craig
Sid Davis
Ila C. Deiss
R. Mark Dietz
Brian M. Doherty
William Domnarski
Robert E. Donlan
Stephen P. Doyle
Michael L. Duncan
Bradley H. Ellis
Gary S. Fergus
Charles S. Frigerio
Michael E. Gabel
Mark E. Goldstucker
Richard J. Goodier
Roger B. Greenberg
Brook Hart
Michael G. Helm
Marland Henderson
Peter E. Heyward
Cathy A. Hinger
Kent S. Hofmeister
William L. Hsiang
Leslie S. Hyman
Frederick S. Jones
Matthew L. Jones
Jeff Keohane
Faye Knowles
Robert C. Knuepfer
Kenneth A. Kraft
Edward G. Kramer
Ramon Lafitte
Merl Ledford
Matthew D. Lee
Eduardo N. Lerma Sr
David E. Leta
Richard D. Lieberman
Gerald A. Lord
Randall J. Love
Joseph H. Low IV
Richard G. MacDougall
Hannah R. Metcalfe
James A. Metcalfe
Christine L. Meuers
Howard A. Meyer
Tom C. Mugavero
Pierre Murphy
Daniel J. O'Brien
Kay Otani
Courtney M. Paulk
Frank A. Perez
Brian W. Plummer
Eli A. Poliakoff
David B. Potter
Roy Pulvers
Rion J. Ramirez
Sandra Rodriguez
Cynthia M. Russo
Jean A. Ryan
Tom Scully
Margaret P. Simmons
Jay Earl Smith
James W. Stewart
Mark R. Strickland
Roger M. Tafel
Mark J. Tamblyn
Charlotte H. Turner
Bruce L. Udolf
Elena Vigil-Farinas
Hon. Alexander P. White
Benjamin V. White
Bradley J. Williams
Kenneth J. Withers
Michael JJ Wolter
Allie M. Wright

Sustaining Members—June
Gil A. Abramson
Ludwig J. Abruzzo
Christian K. Adams
Constance L. Akridge
M. Anne Anderson
Cornwell G. Appleby
Marcia L. Augsburger
Yvette A. Ayala
Michael J. Bagley
John R. Baker
Brian M. Ballay
Robert E. Barkley
Robert E. Barnett
Michael O. Bass
Marylin Batista
Keith J. Bauer
Elizabeth Bazan
Stanley Beutler
Nancy Bloodgood
Eric L. Bloom
Darnell Bludworth
Michelle Blum
Martha Boersch
Daniel Bonnett
Gregory D. Boos
Marie A. Borland
Ann Bowden-Hollis
Richard C. Bradley III
Adam LH Bramwell
Jane Brannon
Damisela C. Brown
Elizabeth J. Brown Fore
Michael P. Brundage
Charles D. Bullock
John Burleson
Joseph P. Busch
Thomas E. Buser
Peter J. Butler
Rex Lamont Butler
George B. Butts
J. Richard Caldwell
Laurence L. Christensen
Lawrence M. Coco
Gregory M. Cokinos
Tim K. Colbert
John David D. Cole Jr
John David D. Cole Sr
Kathryn Collard
Adriana Cortina Martinez
Andrew Cotzin
Robert E. Couhig
Lisa Counters
Paul G. Craig
Joseph A. Curcillo
Daniel E. Danford
Eric B. Darnell
Monica L. Davies
Brian R. Davis
Mark D. DeBofsky
Nuro B. Dedefo
David M. Delaney
Linda R. Dettery
Rajiv S. Dharnidharka
R. Mark Dietz
Brian M. Doherty
William Domnarski
Robert E. Donlan
Stephen P. Doyle
Phillip B. Dye
J. Timothy Eaton
Matthew M. Edwards
Tracey L. Ellerson
Bradley H. Ellis
Charles E. English
Suzanne R. Eschrich
Joseph B. Farrell
Fredrick B. Feeney
Wesley D. Felix
Michael C. Felty
Gary S. Fergus
Wolfgang M. Florin
Charles S. Frigerio
Edward L. Froelich
Cable M. Frost
John Fuentes
Paul J. Galuszka
James B. Geren
Kimberly Gilmour
Gregory A. Giordano
Howard W. Gordon
Robert B. Gough III
Todd P. Graves
Richard R. Gray
Roger B. Greenberg
Robert A. Gualtieri
Carolyn C. Halladay
Joane Hallinan
Stephen C. Hanemann
Brian M. Haney
Christine D. Hanley
Jeanette Hargreaves
Edwin A. Harnden
Brook Hart
Joshua A. Hasko
John C. Henegan
Peter C. Hennigan
Gregory W. Herbert
Edward Hernandez
Peter E. Heyward
Thomas W. Hill
Cathy A. Hinger
Kent S. Hofmeister
Craig F. Holthaus
Dana L. Hooper
James E. Howard
William L. Hsiang
R. Ann Huntrods
Lori L. Jessee
Jack A. Jeziorski
Jeremy C. Johnson
Matthew L. Jones
Brian L. Josias
Claire W. Ketner
John R. Keville
Michael K. Kiernan
Barbara S. Kinosky
Wes A. Kissinger
David T. Knight
Faye Knowles
William J. Kopeny
Kenneth A. Kraft
Jennifer Kroll
Steven D. Kupferberg
Ramon Lafitte
John L. Langslet
Jason D. Lazarus
Merl Ledford
Jack R. Leer
Eduardo N. Lerma Sr
David E. Leta
Richard D. Lieberman
Manuel E. Lopez Fernandez
Gerald A. Lord
Randall J. Love
Joseph H. Low IV
Richard G. MacDougall
Natalie C. Magdeburger
Timothy J. Malloy
Jeffrey E. Mandel
Kevin W. Manning
William D. Manson
Matthew A. Martel
Susan Martin
Philip Marzec
William B. Mateja
James F. Mauro
Rachel K. McCombs
William T. McLaughlin
Maureen McLoughlin
Angus E. McSwain
David R. Melton
Joshua J. Metcalf
Hannah R. Metcalfe
James A. Metcalfe
David C. Mielke
Marshall V. Miller
Steven R. Miller
James A. Minix
Domenique C. Moran
Christopher R. Morris
Pierre Murphy
Jose A. Nazario-Alvarez
Danny M. Newman
Michael P. Nowlan
Daniel J. O'Brien
Catherine R. O'Donnell
Micheal J. O'Shea
Mark R. Osherow
Kay Otani
Diana Lynn Pagan Rosado
Morris R. Parker
Courtney M. Paulk
Lindy L. Paull
David P. Pavlik
Frank A. Perez
John D. Perez
Robert W. Perrin
Anthony J. Piazza
Maryann Pierce Perttunen
Susan D. Pitchford
Mark A. Pivach
Adam D. Pogach
Eli A. Poliakoff
David B. Potter
Teresa Poust
Tony G. Powers
Stephen M. Prignano
Ian D. Prior
George E. Purdy
Rion J. Ramirez
James A. Reeder
Daniel E. Reidy
Tom B. Renfro
James G. Richmond
Ramon Rivera Iturbe
Richard A. Rocap
Kevin J. Rodlund
Carmen-Lucia L. Rodriguez
Luis M. Rodriquez
Sandra Rodriguez
Antonio L. Roig
Danielle E. Rolfes
Cynthia M. Russo
Jean A. Ryan
Ellen C. Sacco
Kenneth L. Sales
Leonard K. Samuels
Jose C. Sanchez-Castro
Benjamin C. Sasse
Karen E. Saul
Jerry K. Sawyer
Barry A. Schultz
Chris M. Schwing
Todd J. Shill
Hon. Houston Shirley
Deanna K. Shullman
Stephen T. Sigler
Michael S. Simon
Laura TD Sims
Richard W. Skillman
Jay Earl Smith
Richard H. Smith
Scott B. Smith
Nicole R. Snapp-Holloway
L. Allan Songstad
Braden W. Sparks
Gerard M. Stegmaier
Paul M. Sterbcow
Karl S. Stern
James W. Stewart
Donald J. Stoecklein
Edwin Sullivan
Kevin R. Sutherland
Roger M. Tafel
Mark J. Tamblyn
John C Tillman
Vincent Tricarico
Charlotte H. Turner
Bruce L. Udolf
Elena Vigil-Farinas
Anthony F. Vittoria
Robert A. von Esch IV
Sharna A. Wahlgren
S. Scott Walker
Robert R. Wallace
Eleanor Warren
Eric S. Waxman
David B. Weaver
Philip B. Whitaker
Hon. Alexander P. White
Benjamin V. White
Glenn M. White
Bradley J. Williams
Steven C. Windsor
Rachel E. Wisley
Michael JJ Wolter
Steven E. Wolter
Brian A. Wood
Douglas H. Wood
Joseph A. Woodruff
Eric Woosley
Allie M. Wright
Benjamin F. Yale
Anne E. Zachritz
Dennis P. Zapka
Charles F. Zimmer
James E. Zloch

New Members—June
Akinyemi T. Akiwowo
William Allred
Kathleen A. Alparce
Mary C. Andrues
Stuart B. Armstrong
Leslie M. Auriemmo
James J. Banks
Ian C. Barras
Brett C. Bartlett
Joy D. Bartscher
Diana C. Bauer
Paul A. Bellin
Bryon J. Benevento
C. Russell Bengtson
Michael A. Bennett
Nicole E. Bergeron
Geoff D. Biegler
Timothy R. Billick
Matthew C. Blickensderfer
Christopher C. Bly
Allen L. Bohnert
Micheal R. Bottaro
Joseph J. Bouldin
Amber N. Bowman
Howard T. Boyd
Lawrence J. Bracken
Hallet R. Brazelton
Joseph R. Brehm
Duncan T. Brown
Timothy D. Brown
Joseph L. Bruemmer
Jacob D. Bundick
Chad Burris
Alison D. Bushnell
Rachel M. Cannon
Jeffrey T. Castellano
R. Glenn Cater

Bryan M. Cavan
Suzanne B. Chanti
William W. Ciesar
Christian J. Clapp
Timothy R. Cleary
Gary O. Cohen
Craig C. Conley
Jude C. Cooper
Kati M. Cox
John T. Culotta
William C. Darrough
Michele H. DeShazo
Nathaniel J. Doan
James E. Dunn
Tanya A. Eades
John E. Egers
Brett D. Ekins
Richard L. Ellison
Stacey G. Evans
Catrina Farrugia
Amy E. Ferber
Brendan J. Flaherty
Robert C. Folland
Marna S. Franklin
Kristine L. Fritz
David M. Gadaleto
Carla Garcia-Benitez
Joseph J. Gavin

Britt M. Gilbertson
Robert M. Gippin
Jeffrey S. Goddess
John S. Godfrey
Dan W. Goldfine
Mary B. Goodman
Joanna M. Greber
Georgann S. Grunebach
Timothy H. Hanna
Brandi Hardin
Janis E. Hawk
Christina Herrera
Jason A. Hill
Keith J. Hilzendeger
Jess M. Hofberger
Colin C. Holley
Maria L. Holmgreen
Matthew C. Hoyer
Joseph L. Hubbard
Virginia Iglesia
Grant W. Jonathan
Kirstin D. Kanski
Sidney W. Kilgore
Danielle M. Kilinski
Benjamin I. Klein
Markus W. Kolber
William J. Kopeny
Edward G. Kramer

Kendall E. Krans
Jeffrey T. Kuntz
Linda G. Lagunzad
Lance J. Lorusso
Klaus D. Luhta
Maureen D. Luke
Alexis MacIvar
Sarah L. McArthur
Heather M. McCann
Alan L. McLaughlin
John H. Metz
Lindsey M. Michon
Robert F. Moorman
William A. Morrison
Blake R. Morrow
Matthew J. Moussiaux
Daniel P. Moylan
Mauricio O. Muôiz-Luciano
Sally R. Murray
Tyler L. Murray
Tibor Nagy
Kerri J. Nelson
Thomas C. Newkirk
Alan Nichols
Edmund J. Novonty
Marc S. Nurik
Stephanie E. O'Byrne
Bradley H. Oliphant

Catherine M. O'Neil
Mark R. Osherow
Paul S. Padda
Thomas M. Parker
Jennifer V. Patricio
Stewart O. Peay
Robert C. Petrulis
Eichorn A. Philip
Eric R. Pierson
William A. Posey
John R. Prairie
Michael B. Quigley
Daniel B. Quon
Jose L. Ramirez
Randall E. Ravitz
Ryan W. Reaves
Walter J. Rekstis III
Matthew J. Richardson
Michael J. Riordan
Debbie E. Rivera
Richard R. Roberts
Erica K. Rocush
Ana M. Santiago-RamÌrez
Gregory C. Sasse
Joseph Schlageter
Sarah R. Shannahah
Kiran Sharma
Robin C. Shaw

Robert T. Sherwin
Sinead C. Soesbe
Susan K. Spurgeon
Paul M. Stoddard
Mario A. Tabone
William F. Taylor
Bart B. Torvik
Colleen D. Truden
Jennifer L. Trupiano-Hill
Peter Turner
H. Hunter Twiford
Robert J. Van Der Velde
Miguel Villarreal Jr
Jessica K. Vllasi
Scott A. Waldron
Patricia M. Ways
Lisa A. Wegner
Kurt Weinreich
Elizabeth R. Wellborn
Nathan Wheatley
Philip R. Wiese
Deborah A. Wilcox
Clairesse N. Williams
Douglas A. Wright
Benjamin F. Yale
James E. Yavorcik

Have you recently moved? Please give us your new address!

For fastest results, please include a copy of your label and mail it to:
Federal Bar Association
Attn: ADDRESS CHANGE
2011 Crystal Drive, Suite 400
Arlington, VA 22202.

Federal Bar Association Membership Application *Raising the Bar to New Heights* TFL-8-07

1. Please tell us about yourself *(Please Print)*

First Name M.I. Last Name

Title

❍ Male ❍ Female Date of Birth / /

First Admission to Bar in U.S. (required, unless applying for law student or foreign associate status)

Court State Bar Date

Please supply both your business and home addresses below.

My preferred mailing address is ❍ Business ❍ Home

Business Address

Firm/Agency

Address

Suite/Floor

City State Zip

( ) ( )
Phone Fax

E-mail

Home Address

Address Apt. #

City State Zip

( ) ( )
Phone Fax

Practice Type *(based on primary employment)*

Private Sector

❍ Government ❍ Judiciary
❍ Military ❍ Non-profit
❍ Association Counsel
❍ University/College

Public Sector

❍ Private Practice
❍ Corporate/In-House

2a. Active Membership *Please choose one.*

	Private Sector	Public Sector
❍ **Member** *Admitted to practice* **0-5 years**	$75	$60
❍ **Member** *Admitted to practice* **6-10 years**	$125	$100
❍ **Member** *Admitted to practice* **11 years or more**	$150	$115
❍ **Retired** *(fully retired from the practice of law)*	$75	$75

2b. Sustaining Membership

❍ *Become a sustaining member today! This optional category is* ***in addition to regular dues****. It is used to support CLE programs & publications.*	$60	$60

2c. Associate Membership

❍ **Foreign Associate** *Admitted to practice law outside the U.S.*	$150	$150
❍ **Law Student Associate** *Currently enrolled in law school*		

Dues Total ..... **$ _____**
Please enter amount in line 4A of the Dues Worksheet.

3. Local Chapter Affiliation, Sections & Divisions

For a complete listing of chapters, sections and divisions, visit www.fedbar.org. Write in chapter, section(s) or division(s), and dues if applicable.

Dues Total ..... **$ _____**
Please enter amount in line 4B of the Dues Worksheet.

4. Dues Worksheet

FBA Dues ..... **4A $ _____**
Local Chapter, Section or Division Dues .. **4B $ _____**
Total Amount Enclosed *(Add 4A, 4B)* ..... **$ _____**

5. Payment Information

Payment Options

❍ Check payable to Federal Bar Association

Please charge my dues to

❍ American Express ❍ Diners Club
❍ Mastercard ❍ VISA

Card No. Exp. Date

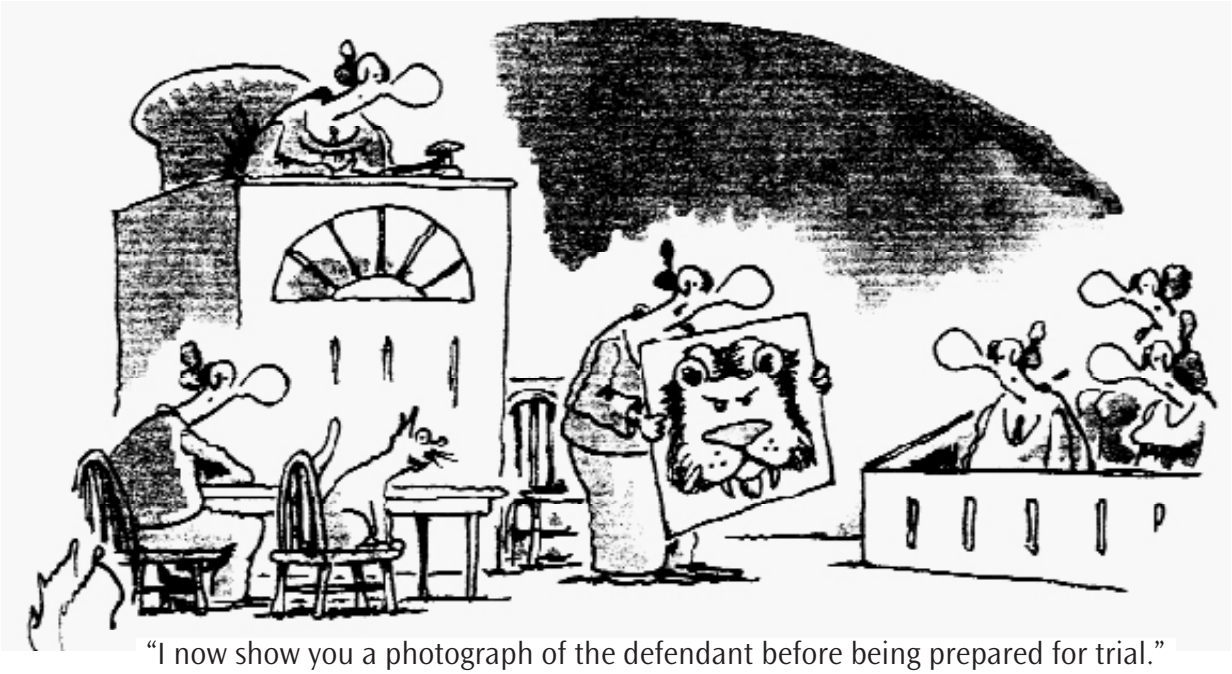
X
Signature Date

The undersigned hereby applies for membership in the Federal Bar Association and agrees to conform to its Constitution and Bylaws and to the rules and regulations prescribed by its National Council.

X
Signature of Applicant *Date*

***Note** *Contributions and dues to the FBA may be deductible by*

Please complete and return to:
FBA Membership Department,
2011 Crystal Drive, Suite 400, Arlington, VA 22202
(703) 682-7000, (703) 682-7001 (fax)
membership@fedbar.org • www.fedbar.org



"I now show you a photograph of the defendant before being prepared for trial."