IADC
International Association of Defense Counsel

The Foundation *of the International Association of Defense Counsel*

One North Franklin, Suite 1205
Chicago, IL 60606
p (312) 368-1494
f (312) 368-1854
e-mail info@iadclaw.org
www.iadclaw.org

IADC

The Joan Fullam Irick

Privacy Project

Phase II

The USA PATRIOT Act: Security and Privacy

Consumer Privacy and Preemption

Constitution, Crime and Clergy

Discovery in Abuse Claims

Parent-Child Communication Privilege

Deliberative Process Privilege

Self Critical Analysis Privilege in Medical Care

European Data Protection

Managing Privacy Risks in Your Business

Confidential Settlement Agreements

Expanding Tort Liability for Information Providers

Romantic Relationships at Work

Funding for the Privacy Project provided by

The Foundation *of the International Association of Defense Counsel*

The Joan Fullam Irick Privacy Project, Phase II

Dedication

This Volume, and its earlier companion (published in January 2003) originated from Joan Fullam Irick's deeply held belief that the very concept of privacy faced challenges on many fronts, in the legislature, in the workplace, and in the courts.

Joan's passion for privacy-related issues led her to devote much of her term as president of the IADC to scrutinizing the many ways that our privacy is being invaded. At her urging, the Foundation of the IADC undertook preparations of scholarly papers analyzing the current state of privacy and anticipating future issues in the area.

Throughout the process that produced these volumes, Joan's commitment to the issues imbued all of us with the desire to create a body of high-level, intellectually rigorous white papers that could be used in many disciplines to continue exploration of privacy issues on both the national and international scene, and the foreseeable future of privacy in the individual and corporate worlds.

Joan Fullam Irick passed away during her term as IADC president. Her youth, her vitality and her grace could not defeat the cancer that ultimately claimed her life. All of us extend our deepest sympathy to her husband, Tom, and their children. Joan's legacy to us survives in this Privacy Project. Joan conceived the project, and she shepherded it through to the end.

In recognition of her efforts, and in gratitude to her service, the Foundation renamed this undertaking the Joan Fullam Irick Privacy Project. We are proud here to dedicate Phase II of that Project to the memory of our former President, the leader who made this all possible, our beloved Joan.

Editors
George S. Hodges, Chair
Jerome A. Galante
Joseph W. Ryan, Jr.

The Joan Fullam Irick Privacy Project, Phase II

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

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

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

In January 2003, Phase I of the Privacy Project was published as a dedicated issue of the IADC Defense Counsel Journal. It was met with repeated positive critiques and commentary from IADC members.

With the support of then President Irick, a decision was made to proceed ahead into Phase II, exploring new areas of concern in the world of privacy while revisiting and updating some of the earlier topics. The within Volume is the end result of this decision.

The Privacy Project editorial team thanks the authors for their commitment and dedication to this project. The talent and dedication of these individuals form the cornerstone of this publication and devotion to the privacy principles espoused by Joan.

The editorial team also thanks Pam Miczuga and Mary Beth Kurzak of the IADC staff, whose multi-task efforts made this project possible, and IADC Executive Director Oliver Yandle for his thoughtful suggestions and input. Finally, the editorial team thanks Joan Irick, whose spirit will live on with us as the Privacy Project moves ahead.

Table of Contents

The USA PATRIOT Act: Tensions Between Security and Privacy
By Robert A. Curley, Jr. and Lisa M. Caperna.....1

Consumer Privacy and Preemption: An Overview of Gramm-Leach-Bliley, the Fair Credit Reporting Act and Proposed 2003 Legislative Amendments
By Virginia N. Roddy.....13

Protection Against Discovery in Civil and Criminal Proceedings in Clergy Sexual Abuse Claims
By Ralph M. Streza and L. Gino Marchetti, Jr......23

Personnel Records, Pedophiles and Priests: An Addendum to Discovery in Sexual Abuse Claims
By William G. Porter II and Michael C. Griffaton.....35

Family Unity or Family Crisis: Revisiting the Need for a Parent-Child Communication Privilege
By Mark D. Fox and Michael L. Fox.....41

The Deliberative Process Privilege: What Is It? When Can It Be Asserted? How Can This Shield Be Pierced?
By Cathy Havener Greer, William T. O'Connell and Kristin J. Crawford.....55

The Self Critical Analysis Privilege in Medical Care: The Law is One Thing in Rome and Another In Athens
By Paul E. Svensson and George S. Hodges.....69

European Data Protection: Impact on U.K.-U.S. Data Transfers
By Ian MacDonald and Julia Graham.....81

Managing Privacy and Security Risks in Your Business: Are You Properly Protected?
By Kathy J. Maus, Michael G. Haire, Jr. and Emily Freeman.....89

How Good is Your Confidential Settlement Agreement?
By William B. Crow.....105

Expanding Tort Liability of Information Providers: How Far Can Foreseeability Be Stretched?
By Dennis T. Ducharme.....113

Romantic Relationships at Work: Does Privacy Trump the Dating Police?
By Rebecca J. Wilson, Christine Filosa and Alex Fennel.....121

IADC
International Association of Defense Counsel

Privacy Project Editors
George S. Hodges, Chair
Jerome A. Galante
Joseph W. Ryan, Jr.

The Foundation
of the International Association of Defense Counsel

The USA PATRIOT Act: Tensions Between Security and Privacy

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

I. Introduction

On the morning of September 11, 2001, Americans watched - over and over - the news footage of airplanes crashing into the World Trade Center in New York City; they were shocked. Less than an hour later, they watched an airplane destroy a portion of the Pentagon; and by then, they knew their world would never be the same. No enemy had ever invaded this nation in such a horrific manner prior to the day which is commonly referred to as simply 9/11.

One day after the terrorist attacks, President George W. Bush vowed that "we will not allow this enemy to win the war by changing our way of life or restricting our freedoms." Less than six weeks after the attacks, The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (better known by its catchy acronym, the USA PATRIOT Act) was endorsed by Congress and signed into law by President Bush on October 26, 2001.

The USA PATRIOT Act is a sweeping piece of legislation making changes to more than fifteen different statutes, including the Foreign Intelligence Surveillance Act of 1978 ("FISA"), the Electronic Communications Private Act of 1986 ("ECPA"), and the Family Education Rights and Private Act ("FERPA") with potential implications for the protection of civil liberties.

Attitudes toward increased police power and surveillance have changed in the wake of the September 11th attacks. A CBS/New York Times poll conducted in September 2001 asked respondents whether American's had to give up some personal freedoms in order to make the country safe from terrorist attacks. Seventy-nine percent replied: yes. Those in favor of expanded police power call for legislation that would allow government agencies more effective means to combat terrorist networks. They argue that many of the changes resulting from the USA PATRIOT Act simply recognize modern technological innovations and allow the government to adapt their practices to such technology.

Other political activists, however, have criticized the Act, arguing that it gives the Attorney General and federal law enforcement unnecessary and permanent new powers to violate civil liberties that go far beyond the stated goal of fighting international terrorism. Their worry is that these new and unchecked powers could be used against American citizens who are not

Robert A. Curley, Jr. graduated from Harvard College and Cornell Law School and is the President of Curley & Curley P.C. in Boston. Mr. Curley is a past President of the Massachusetts Defense Lawyers Association and is the Massachusetts State Representative to the Defense Research Institute. He currently serves on the Board of the IADC Foundation and has served on the faculty of the IADC Trial Academy in 1999. Mr. Curley concentrates his practice in the area of catastrophic personal injury, product liability, and insurance coverage matters.

Lisa M. Caperna is a graduate of Boston College, magna cum laude and Boston College Law School. Ms. Caperna is presently an associate at Curley & Curley P.C., where she concentrates her practice in general civil litigation and defense of government agencies.

under criminal investigation and those whose First Amendment activities are deemed to be threats to national security by the Attorney General.

So, should we be concerned? Is the USA PATRIOT Act necessary to national safety given the modern technology of the 21st Century? Or does the Act go too far, allowing the government to compromise cherished rights which we have enjoyed and on which our country prides itself? If so, are we willing to accept that compromise? Before we answer this question, we should keep in mind what Benjamin Franklin had to say on the subject...

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." (Inscribed on the pedestal of the Statute of Liberty)

It is difficult to estimate the impact of the USA PATRIOT Act because its provisions modify more than fifteen existing statutes. The bill itself is over 342 pages long and must be read together with the existing statutes to understand the significance of its language. To better understand the impact of this Act, it is helpful to review the evolution of law concerning the balance between protecting privacy and allowing government to fight crime, beginning with early case law and extending to the statutory environment at the time the USA PATRIOT Act was enacted.

II. The Tensions in Government Powers to Provide Security and Privacy

The inherent tensions between government action to protect the security of the people and to protect individual rights, including privacy, have always existed in our republic. The preamble to the Constitution of the United States succinctly describes this tension in expressing the rationale for the Constitution itself, namely to,

> . . . establish Justice, insure domestic Tranquility, provide for the Common Defense, promote the general Welfare and secure the Blessings of Liberty . . .

Alexander Hamilton argued that the "principal purposes to be answered by union are these - the common defense of the members; the preservation of the public peace, as well against internal convulsions as external attacks." In discussing the authorities essential to the common defense, Hamilton stated, "These powers ought to exist without limitation, because it is impossible to foresee or to define the extent and variety of the means which may be necessary to satisfy them." (emphasis in original).[1] Hamilton did not favor a separate Bill of Rights.[2] Hamilton did foresee that "unjust and partial laws" which affected "the private rights of particular classes of citizens" could be passed by legislatures. He stressed the "vast importance" of the judiciary "in mitigating the severity and confining the operation of such laws."[3]

The People clearly saw the wisdom of a Bill of Rights for the protection of individual liberties and rejected Hamilton's view that a Bill of Rights was unnecessary.

Present considerations of the powers of government to secure our defense in present day national exigencies of increasingly unforeseeable extent and variety, the vast importance of our independent judiciary and the rights of individuals are, in essence, the same considerations present at the birth of our nation. Our people will probably always possess nearly unanimous accord on the goals of security and the protection of personal rights and privacy, but will probably always disagree and debate about the necessary balance to be achieved among the means to achieve those goals.

III. Traditional Concepts of Limitations on Government Intrusion Into Privacy

A. The Fourth Amendment

The strongest protection Americans have against unreasonable governmental intrusions into their privacy is the Fourth Amendment, which provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unrea-

1. The Federalist No. 23, The Federalist, 2000 Modern Library Edition, p. 140.
2. The Federalist No. 84, op cit., pp. 546-557.
3. The Federalist No. 78, op cit. p. 501.

sonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[4]

Early interpretations of the Amendment focused on privacy as a property concept. Relying on this concept in cases concerning electronic surveillance such as *Olmstead v. United States*, the Supreme Court upheld the unwarranted wiretaps in question and refused to extend the Fourth Amendment language to include telephone wires.[5]

Olmstead challenged his conviction of conspiracy to violate the National Prohibition Act on the basis that the use of evidence of private telephone conversations, intercepted by federal agents through wiretapping, amounted to a violation of the Fourth Amendment.[6] The Court reasoned that there could be no search when there was no physical invasion of the appellant's personal space, and likewise there could be no seizure given that words are not tangible things capable of being seized.[7] Justice Brandeis's dissent, however, signaled a shift in attitude away from such unyielding property-based applications of the Fourth Amendment when he stated:

> "The makers of our Constitution... sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone...To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[8]

Thirty-nine years after *Olmstead*, the court again faced an electronic surveillance issue in both *Berger v. New York* and *Katz v. United States*.[9] In Berger, the Supreme Court struck down a New York statute authorizing electronic eavesdropping by law enforcement officials investigation certain types of crimes. The Court held that conversations fall within the meaning of the Fourth Amendment, and that the seizure of conversations constitutes a Fourth Amendment search.

Furthermore, the Court stated that evidence obtained by surveillance conducted in violation of the Fourth Amendment is inadmissible in court. Concluding the statute was so broad that it failed to meet constitutional standards under the Fourth Amendment, the Court delineated the constitutional criteria that electronic surveillance legislation should contain.[10] The Court held that the Fourth Amendment requires that a search warrant describe with particularity the person, place or thing to be seized, the nature of the crime in question and the type of conversation sought. The Berger Court maintained that the continuance of surveillance should be permitted only upon renewed showings of probable cause. The Court also stated that there should be "precise and discriminate" procedures in place to minimize the unauthorized interception of conversations unconnected to the crime being investigated.

In *Katz*, FBI agents - acting without a warrant - set up a wiretap by attaching a listening device to the outside of a public telephone booth from which the appellant was engaging in illegal bookmaking activities.[11] In the landmark case, the Court ruled that "the Fourth Amendment protects people, not places." Justice Harlan's concurring opinion set forth a two-part test used to determine whether a search or seizure is reasonable.[12] First, the court must decide whether the individual had a subjective expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable.[13] Furthermore,

4. U.S. Const. amend. IV.
5. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).
6. *Id.* at 455.
7. *Id.* at 464.
8. *Id.* at 478 (Brandeis, J., dissenting).
9. Berger v. New York, 388 U.S. 49 (1967); Katz v. United States, 389 U.S. 347 (1967).
10. *See* Berger, *supra* at 54-64.
11. *See* Katz, *supra* at 348.
12. *Id.* at 361 (Harlan, J., concurring).
13. *Id.* at 358, n.23.

the Court concluded that the agents failure to obtain prior judicial approval was "per se unreasonable under the Fourth Amendment."[14]

In dicta, the Court recognized the possibility that in matters of national security, prior authorization for electronic surveillance may not always be required, limiting its decision to issues of domestic criminal surveillance only.[15]

The Court finally addressed the relationship between issues of domestic and national security and electronic surveillance in 1972, in *United States v. United States District Court (Keith)*, in which the defendants were charged with conspiracy to destroy government property.[16]

Specifically, one defendant was charged with the attempted bombing of a CIA recruiting office in Michigan. The Court held that the warrantless electronic surveillance of a domestic organization with no alleged connection to a foreign government constituted a breach of Fourth Amendment protections. The Court left open the possibility of different Fourth Amendment standards for national security investigations involving foreign organizations.[17] Eerily foreshadowing Congress' future expansions of electronic surveillance, Justice Powell stated,

"Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent."[18]

B. The First Amendment

The First Amendment provides that "Congress shall make no law respecting the establishment of religion, or prohibiting the free exercise thereof: or abridging the freedom of speech, or of the press: or the right of people peaceably to assemble, and to petition the Government for a redress of grievances."[19]

In general, the First Amendment prevents government from proscribing speech, expressive conduct or association because of disapproval of the ideas expressed or believed. While many forms of expressive activities are protected by the First Amendment, the courts have allowed little to no protection for those who seek to incite violence, or who use violence or otherwise illegal acts as a means of protest. For example, in *NAACP v. Claiborne Hardware Co.*, the Supreme Court declared "violence has no sanctuary in the First Amendment, and the use of weapons, gunpowder, and gasoline may not constitutionally masquerade under the guise of 'advocacy'."[20]

Since violence or illegal acts are not protected under the right of free expression, the First Amendment will not act as a barrier against government surveillance of such activities. Yet, where individuals exercise free expression in a manner protected by the First Amendment, the courts have recognized that the First and Fourth Amendments are meant to protect against government surveillance targeted specifically at such behavior. In *United States v. United States District Court*, the Court stated that "history abundantly documents the tendency of Government - however benevolent and benign its motives - to view with suspicion those who most fervently dispute its policies."[21]

IV. The Threats Presented by 21st Century Terrorism and Crime

On February 26, 1993, six people were killed and more than 1,000 injured when terrorists bombed the World Trade Center in New York City.[22] On April 19, 1995, 168

14. *Id.* at 359.
15. *See id.*
16. United States v. United States District Court, 407 U.S. 297, 299 (1972).
17. *Id.* at 321-22, 324.
18. *See id.* at 313-315.
19. U.S. Const. Amend. I.
20. NAACP v. Claiborne Hardware, 458 U.S. 886, 916 (1982).
21. Keith, *supra* at 314.
22. CNN Interactive, Last World Trade Center bombing conspirator sentenced, at http://www.cnn.com/US/9804/03/wtc.bombing (last visited August 12, 2003).

people, including 19 children, were killed when a car bomb exploded in front of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma.[23] On August 7, 1998, 223 people were killed in the bombing of United States embassies in Nairobi, Kenya and Dar es Salaam, Tanzania.[24] On October 12, 2000, a suicide bomber rammed into the side of the Navy destroyer USS Cole, killing 17 and wounding 40.[25] And on September 11, 2001, terrorists hijacked four planes, crashed one plane into each tower of the World Trade Center, another into the Pentagon and the fourth, believed to be headed toward a target in the nation's capital until passengers and its crew diverted the plane, into a field in western Pennsylvania.[26] Approximately 3,062 people were killed in those attacks.[27] These tragedies represent only a sample of the terrorist attacks which have plagued the past decade alone and have had the greatest affect on America.

V. Pre-USA PATRIOT Act Surveillance Law

A. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)

Title III was the legislative response to the Supreme Court's decision in both *Berger* and *Katz*, where the Court laid out constitutional standards for electronic surveillance. In enacting Title III, Congress sought to regulate the use of electronic surveillance as an investigative tool and the disclosure of materials obtained through such surveillance. In enacting Title III, Congress also sought to protect privacy by establishing a rigorous set of requirements for how such surveillance could be conducted. By incorporating the criteria set forth in Berger and Katz, Congress created a strict standard for surveillance that extends the requirements of the Fourth Amendment.

Title III authorizes law enforcement to engage in surveillance activities pursuant to a court order based on a finding of probable cause that a serious crime has been or is about to be committed, and award of a warrant - in compliance with Fourth Amendment directives.[28] Title III also requires a showing of necessity and minimization. For example, law enforcement may not resort to electronic surveillance unless normal investigative procedures have either failed or are too dangerous.[29]

Additionally, surveillance must be conducted in a timely manner so that interceptions of communications, not otherwise subject to surveillance, are minimized.[30] In emergency situations, however, where there is immediate danger of death or serious injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime, warrantless wiretapping is permitted, so long as an application for a warrant is made within 48 hours of the commencement of interception.[31]

Congress repeatedly amended Title III to keep up with constant advances in technology. In response to the increase use of computers, e-mail, cellular telephones, internet providers, and other forms of communication technology, Congress amended Title III by passing the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA made Title III applicable to, inter alia, voice mail and e-mail messages.)

B. Foreign Intelligence Surveillance Act of 1978 (FISA)

As Title III and ECPA authorizes electronic surveillance only in criminal cases,

23. CNN Interactive, *Oklahoma City Tragedy: The Bombing*, at http://www.cnn.com/US/OKC/bombing.html (last visited August 12, 2003).

24. Office of International Information Programs, U.S. Department of State, *Fact Sheet: Terrorist Bombing of U.S. Embassy in Kenya* at http://usinfo.state.gov/regional/af/security/a0081101.htm (last visited August 12, 2003).

25. Wendi S. Ross, *Ashcroft Announces Indictment of Two in USS Cole Bombing*, (last modified May 15, 2003) at http://usinfo.state.gov/topical/pol/terror/texts/03051502.htm (last visited August 12, 2003).

26. Office of International Information Programs, U.S. Department of State, *A Selected Chronology of Key Events, September 11, 2001* -Present at http://usinfo.state.gov/journals/itgic/0902/ijge/gjchron.htm (last visited August 12, 2003).

27. *Id.*

28. 18 U.S.C. 2518(3)(a) (2000).

29. *Id.* at 2518 (3)(c).

30. *Id.* at 2518 (5).

31. *Id.* at 2518(7).

Congress determined that similar legislation authorizing electronic surveillance for foreign intelligence gathering purposes was necessary as threats to national security increased. FISA allows wiretapping of aliens and citizens of the United States when there is probable cause to believe that the target of the wiretap is a member of a foreign terrorist group or an agent of a foreign power. FISA seeks to deter espionage within the United States by a foreign government or component thereof, by any entity that a foreign government acknowledges it controls and directs, and by any group engaged in international terrorism.[32]

FISA requires that a federal official, with the approval of the Attorney General, submit an application for electronic surveillance warrants to the Foreign Intelligence Surveillance Court (FISC). The application must include: the identity of the target, the information indicating probable cause to believe that the target is a "foreign power" or an "agent of a foreign power," evidence that the location indicated for surveillance is being used or is about to be used by the target, the type of surveillance, proposed minimization procedures, and certification that the information sought is "foreign intelligence information."[33]

Such requirements do not rise to the level of the Fourth Amendment's probable cause requirement in a criminal investigation. Probable cause in a criminal investigation exists "where facts and circumstances within their [the officers'] knowledge... are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed."[34] Congress' justification for the less stringent requirements found in FISA is that the officer is not seeking evidence of criminal activities on which to base a prosecution, but rather is seeking information regarding foreign intelligence activities that may compromise national security.

It is important to note that once the Attorney General certifies the application of a federal officer, the surveillance request is "subjected to only minimal scrutiny by the courts."[35] In fact, on April 29, 2003, the Attorney General reported that 1,228 applications were made to the FISA court for either electronic surveillance or physical searches during calender year 2002 and all of these applications were ultimately approved.[36]

In emergency situations, FISA permits the Attorney General to authorize warrantless searches for a 24-hour period when the Attorney General certifies that an emergency situation exists requiring immediate surveillance. Furthermore, warrantless searches are allowable for periods of up to one year when the Attorney General designates a situation an "emergency," as long as such surveillance is demonstrated, in writing, to be solely directed at communication between or among foreign powers. Such provisions raise another concern; namely, that the Attorney General may declare any situation an "emergency," as the statute does not define what constitutes an emergency.

Information obtained under FISA's provisions could be disclosed for law enforcement purposes if either the information was to be used in a criminal proceeding and the Attorney General had given advanced authorization, or if the government could establish that intelligence gathering had

32. 50 U.S.C. 1804, 1823 (2000).

33. *Id.* at 1801(e).

34. Brinegar v. United States, 338 U.S. 160, 175-76 (1949). However, when the subject is a U.S. person, a higher probable cause standard is imposed and the application must show that the acquisition of such information is necessary to national defense or security or the conduct of foreign affairs. In the case of a non-U.S. person, it is sufficient to show that the information to be acquired is merely related to the national defense or security or the conduct of foreign affairs. Nat'l Security Agency, *NSA Report to Congress: Legal Standards for the Intelligence Community in Conducting Electronic Surveillance (2001)*, at http://www.fas.org/irp/nsa/standards.html (last visited August 13, 2003).

35. United States v. Duggan, 743 F.2d 59, 77 (2nd Cir. 1984).

36. *See* Report from John Ashcroft, Attorney General, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (Apr. 29, 2003). This disclosure was made pursuant to 50 U.S.C. § 1807, which requires that such a report be provided in April of each year.

been the "primary purpose" of the surveillance.[37]

Proceedings of the FISC are conducted in secrecy due to national security concerns. Where the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, 1806(b) of FISA provides for in camera, ex parte review of the application by the court. Unlike Title III which provides for disclosure of Title III applications made and orders granted upon a showing of good cause by the target, FISA does not provide a similar privacy protection to targets. This practically ensures that intrusive wiretaps that do not uncover incriminating information, and thus do not result in prosecutions, never will be made known to the target.

VI. Provisions of the USA PATRIOT Act Relating to Government Intrusions Into Privacy

A. Definition of Domestic Terrorism

Section 802 of the Act amends the criminal code, 18 U.S.C. 2331, to add a new definition of "domestic terrorism" to include activities that: (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by mass destruction, assassination, or kidnapping; or (iii) to effect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States. Such extensions of the definition of terrorism threatens to transform conduct that was once thought of as freedom of expression or freedom of association designed to influence government policy into a terrorist act.

37. *E.g.*, United States v. Pelton, 835 F.2d 1067, 1076 (4th Cir. 1987); United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987) (finding no merit to petitioner's contention that he was entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance).

B. Section 218: Elimination of the Primary Purpose Standard of FISA

Section 218 of the USA PATRIOT Act relaxes FISA requirements permitting the issuance of FISA warrants where foreign intelligence is a "significant" - though not necessarily the "primary" - purpose of an investigation. By requiring that the primary purpose of a wiretap or search was to obtain foreign intelligence, FISA forbade the use of the surveillance authority in criminal cases without meeting the Fourth Amendment probable case standard. As the Act does not provide a definition of "significant purpose," it is unclear how far the FISC will stretch its interpretation of this phrase to accommodate law enforcement and intelligence agencies.

The modification has been criticized for making it easier for the government to circumvent what are supposed to be limitations on permissible domestic surveillance. This potential end-run around Title III's Fourth Amendment's probable cause requirement for criminal investigations contradicts the rationale for permitting a lower threshold for obtaining FISA wiretaps. The consequences of this amendment to FISA may mean that surveillance authority for investigations seeking information primarily pertaining to purely domestic criminal activities will be granted without a showing of probable cause that a serious crime has been or will soon be committed.

Courts, however, may limit the potential reach of Section 218. For example, the court in *United States v. Troung Dinh Hung* held that "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution."

While Section 218 may be vulnerable to constitutional challenge, it is still an expansion of government intrusion into privacy, albeit in the interest of protecting national security.

C. Section 206: "Roving" Surveillance

Section 206 of the USA PATRIOT Act extends Title III's roving wiretap authority to intelligence wiretaps authorized under FISA. The government now has the power to intercept all of a suspect's wire or electronic communications relating to the conduct under investigation, regardless of the suspect's location when communicating. The result is that surveillance can follow a person, rather than requiring a separate court order identifying each telephone company or other communication carrier whose assistance is needed.

Advances in technology certainly justify modifying FISA to allow intelligence surveillance to meet the growing use of cellular telephones, pages, e-mails and other portable methods of communication so that surveillance may continue without disruption when, for instance, a suspect changes cell phone numbers. Section 206, however, does not extend Title III's "reasonably proximate" provision to FISA wiretaps. Such provision requires law enforcement to demonstrate that the target actually uses the device to be tapped.

The extension of roving wiretap authority to FISA without the "reasonably proximate" provision of Title III raises the concern that innocent individuals could have their privacy invaded. Pursuant to a FISA warrant, an agent can listen to a phone line in an innocent person's home for an entire day, if the agent had information that the target was expected to visit that person at some point during a given twenty-four hour period. Even if it is clear that the target already had left the location, the surveillance can continue. Given the lower standard of proof required to obtain a FISA warrant in the first place, the potential for such an invasion into an innocent person's privacy seems all the more likely.

This provision will sunset on December 31, 2005 providing an opportunity for debate on whether such surveillance should continue or not.

D. Section 213: "Sneak and Peek" Warrants

Section 213 of the USA PATRIOT Act permits agencies to execute so-called "sneak and peek" warrants without notifying the target of the search until completion of the search. Usually notice is required when agents conduct a search, except in very specific circumstances when authorities must obtain judicial permission to delay notification. Section 213 allows law enforcement agents to delay notification in every criminal case.[38]

The Supreme Court has held that a search and seizure of a dwelling may be constitutionally defective if police officers enter without prior announcement. This requirement is codified in the federal criminal procedure statutes and is referred to as the "knock and announce" protocol. Section 213 amends FISA by adding a new subsection, 18 U.S.C. 3103a(b), which provides that the requisite notice of the issuance of any warrant (under any provision of law) may be delayed if the court has reasonable cause to believe that the immediate notification of execution of the warrant will have an "adverse effect." The warrant need only provide for giving notice "within a reasonable period of its execution," and the period my be extended for "good cause."

Moreover, while Section 213 stipulates that warrants issued under the delayed notice provision prohibit seizure of tangible property, communications, or electronic data, such as e-mails or voice mails, this requirement may be waived if the court finds "reasonable necessity for the seizure."

The result of Section 213 is that individuals are not provided with notice of a search and, therefore, have no opportunity to check if the warrant is valid or even accurate for that matter. Consequently, an individual may come home and find their personal belongings missing and have no idea what happened to their things. Weeks or even

38. On July 22, 2003, the U.S. House of Representatives in an overwhelming bipartisan effort agreed to an amendment that would effectively prohibit any implementation of Section 213. The Otter Amendment, added to the Commerce, Justice and State Departments funding bill and named after Rep. C.L. "Butch" Otter, an Idaho Republican, passed by a margin of 309 to 118, with 113 Republicans voting in favor. The amendment still has to make it pass the Senate and President Bush before it becomes law.

months later they may receive a letter in the mail explaining that their home was searched and property seized. The individual may then realize that the police had someone else's name matched with their address. Another possibility, is that law enforcement may be entering and searching homes but not seizing anything, leaving no indication that they were ever there in the first place.

If you think these changes will not affect you because you're not involved with terrorist activity, you may be in for a big surprise and an empty house one day. This delay notification is not limited to investigations of terrorist activity. In fact a delayed notice warrant can be justified by simply demonstrating that an individual is "seriously jeopardizing an investigation or unduly delaying a trial."[39](e) otherwise seriously jeopardizing an investigation or unduly delaying a trial. What does that mean? Who knows.

E. Sections 214 and 216: FISA Pen Register and "Trap and Trace" Orders

Section 214 expands the definition of pen register and trap and trace devices to encompass communications from the Internet, including electronic mail and Web surfing. A pen register is a device that registers and records all telephone or Internet service provider numbers dialed by a phone for outgoing communications. A trap and trace device similarly registers numbers of telephones or Internet service provider numbers dialing in.

Previously, under FISA, law enforcement was able to obtain a pen register or trap and trace order requiring a telephone company to reveal the numbers dialed to and from a particular telephone. Now, pursuant to Section 214, law enforcement can utilize pen register and trap and trace under FISA orders to obtain Internet communications in any investigations "to protect against international terrorism or clandestine intelligence activities," provided that such investigation of a Unites States person is not conducted solely upon the basis of activities protected by the First Amendment.

This expansion of the use of pen register and trap and trace devices raises privacy concerns. The previous use of pen register and trap and trace devices to obtain telephone numbers did not reveal the content of any conversation occurring at those telephone numbers. Because very little is revealed, the standard of proof required for this type of warrant is very low: "relevant to an ongoing criminal investigation."

Internet service provider numbers, however, contain data that is far more revealing than telephone numbers. Through the use of trap and trace devices, law enforcement can determine which websites a person visits and view subject lines of e-mail communications, which is equivalent to obtaining content, while only having to demonstrate the low standard of proof required under FISA.

Section 216 expands the range of FISA pen register and trap and trace authority to "anywhere in the United States." Formerly, the order was limited to the jurisdiction of the court to a particular communications provider or location. Now, the order follows the FBI and the suspect anywhere. Thus, law enforcement officers no longer have to seek orders from multiple courts in the course of a large-scale investigation. Like the roving surveillance powers, this raises concerns relating to identification of the party charged and the practical ability to challenge the order.

F. Section 215: Access to Business Records

Section 215 expands the business records seizures available under a FISA order to allow law enforcement agents to compel the production of "any tangible things" (i.e., books, computers, disks and records) sought for an investigation "to protect against international terrorism or clan-

39. 18 U.S.C. 2705 (1995). The definition of "adverse result" is borrowed from another provision of the code which includes the following as "adverse results" justifying delayed notice:
(a) endangering the life or physical safety of an individual;
(b) flight from prosecution;
(c) destruction of or tampering with evidence;
(d) intimidation of potential witness; or

destine intelligence activities." The government need only specify that the records sought contain foreign intelligence information not concerning a U.S. citizen or permanent resident, or that the records are needed to protect against international terrorism. In addition, the Act states that, "no person shall disclose to any other person...that the Federal Bureau of Investigation has sought or obtained tangible things under this section." The extension of searches is not limited to foreign powers and their agents and may include U.S. persons, as long as the investigation is relevant to an investigation and "not conducted solely upon the basis of activities protected by the First Amendment." This provision also will sunset on December 31, 2005.

G. Section 507: Required Disclosure of Educational Records

Congress passed the Family Educational Rights and Privacy Act (FERPA) in 1974 to protect the privacy rights of students and their parents with respect to their educational records. The Act provides that no funds will be made available to an educational institution that permits the release of educational records of its students (or personally identifiable information beyond directory information contained in a record) except where the release is authorized b the student or by statute.[40]

Pre - Section 507, FERPA permitted disclosure of educational records to law enforcement pursuant to a subpoena, based upon probable cause and a sworn affidavit demonstrating that the information sought was probative of a criminal investigation. Section 507 amended FERPA to require automatic disclosure of such records to federal law enforcement upon an ex parte court order based only upon certification that the educational records may be relevant to an investigation of domestic or international terrorism.

H. Section 358: Bank Secrecy Provisions and Activities of Unites States Intelligence Agencies to Fight International Terrorism

Section 358 amends the Right to Financial Privacy Act of 1978[41] to allow law enforcement authorities to obtain financial data related to intelligence or counterintelligence activities, investigations, or analysis in an effort to protect against international terrorism. Thus, financial analysis is now a sufficient basis for federal authorities to review citizen financial information. Further, Section 358 allows government investigators access to consumer records without a court order. The records are to be provided in secret and without civil liability.

VII. Provisions of the USA PATRIOT Act Which Protect Privacy

A. Section 212: Emergency Disclosure of Electronic Communications to Protect Life and Limb

Section 212 provides for voluntary and required disclosure of customer information from Internet Service Providers (ISPs) only during emergencies. Section 212 permits ISPs to disclose the content of stored e-mail messages and other customer information to a governmental entity without first contacting the customer, if the provider "reasonably believes that an emergency involving the immediate danger of death or serious physical injury" justifies disclosure of the information[42]. Pursuant to Section 212, ISPs can disclose information not only to governmental entities but to virtually "anyone" incident to the emergency.

Pursuant to Section 212, an owner or operator of a computer network may now authorize law enforcement to intercept a computer trespasser's wire or electronic communication on the network where the communications will be relevant to an investigation and the interception does not acquire communications other than those

40. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2000).

41. 12 U.S.C.S. 3412 (1978)

42. In the case of records revealing cable subscriber selection of video programming from a cable operator, the ISP must first contact the customer.

transmitted to or from the computer trespasser. Thus, companies, universities, or other computer system operators can now obtain assistance from law enforcement authorities when they come under attack from trespassing hackers. This eliminates the need for law enforcement to first obtain a court order before performing the surveillance activities now authorized under this provision.

Providers complying with a government order in good faith are immune from liability to third parties. Providers who turn over records or communications voluntarily under Section 212, though not expressly immunized from third-party liability in the USA PATRIOT Act, should enjoy such immunity under the Electronic Communications Privacy Act.

This amendment will sunset on December 31, 2005.

B. Section 223: Civil Liability for Certain Unauthorized Disclosures

Section 223 allows court action against government agents who violate prohibitions against the unauthorized release of information that the government obtains through surveillance and increases the ability of the government to discipline employees who commit such violations. This section further calls upon the Inspector General of the Department of Justice to review information and receive complaints alleging abuse of civil rights and civil liberties by employees and officials of the Department of Justice.

C. Section 326: Verification of Identification

Section 326 requires financial institutions to adopt procedures for verifying the identity of new customers. Section 326 requires the Treasury to issue regulations for financial institutions setting forth minimum standards for customer identification when opening an account. The regulations require verification of customer identification, maintenance of records of verification, and comparison of identification with government lists of known or suspected terrorists.

D. Section 362: Establishment of Highly Secure Network

Section 362 directs Treasury to establish within its Financial Crimes Enforcement Network a highly secure electronic network through which reports - including Suspicious Activity Reports (SARs) - may be filed and information regarding suspicious activities warranting immediate scrutiny may be provided to financial institutions.

VIII. Judicial Treatment of the USA PATRIOT Act

In *Global Relief Foundation, Inc. v. Paul H. O'Neill, et al*, 207 F. Supp. 2d. 779 (N.D. Ill. 2002), the Global Relief, an Islamic charitable organization, challenged the constitutionality of a search performed by the FBI of Global Rights headquarters and the home of its president. The Court reviewed the materials seized in camera and ex parte, and affirmed the constitutionality of the search. The Court expressed considerable deference to judicial intervention in the conduct of foreign policy by the Executive Branch. The Court found probable cause and proper compliance by the government with FISA. The Court held that the USA PATRIOT Act had expanded the International Emergency Economic Powers Act so that the President could block the exercise of property rights during an investigation with respect to "any property in which any foreign country or a national thereof has any interest by any person . . . subject to the jurisdiction of the United States."[43] Two of Global Relief's three directors were foreign nationals, and the Court upheld the blocking order in issue with respect to domestic assets of Global Relief.

The Court held that Global Relief did not have a likelihood of success on the merits with respect to constitutional challenges to the USA PATRIOT Act based on theories that it violated the Bill of Attainder clause, the Ex Post Facto clause, the Takings clause

43. 207 F. Supp. 2d at 793.

of the Fifth Amendment, the Due Process clause of the Fifth Amendment, violation of the Fourth, Fifth and Sixth Amendments, and that it was unconstitutionally vague.

In *United States v. Richard C. Reid*, 206 F. Supp. 2d 132 (D. Mass. 2002), Reid moved to dismiss one count of a multiple count indictment against him for an alleged attempt to explode a shoe bomb on a plane on grounds that §801 of the USA PATRIOT Act[44] did not apply to airplanes. The section applied to mass transportation vehicles. The Court held that airplanes were involved in mass transportation, but held that an airplane was not a "vehicle" for the purposes of that section. The Court noted that Reid was facing charges under other Federal laws which specifically applied to airplanes.

In *American Civil Liberties Union v. U.S. Department of Justice*, 265 F. Supp. 2d 20 (DDC 2003), the ACLU sought information from the government concerning the number of times the Department of Justice used the surveillance and investigatory tools authorized by the USA PATRIOT Act. The Court granted summary judgment to the government, holding that it had sustained its burden of establishing that the information sought was properly within the national security exemption to the Freedom of Information Act.

In *Stoutt v. Rancal International, Inc.*,45 the Plaintiffs brought claims for malicious prosecution, unlawful arrest and incarceration, and defamation arising out of a report of suspected illegal activity. Summary judgment entered in favor of the bank which had reported possibly illegal check kiting activities. The bank was immune from liability to the Plaintiffs on the basis of the safe harbor provisions of the Wiley Anti-Money Laundering Act[46], as amended by the USA PATRIOT Act. The court observed:

> Assuredly, under the safe harbor provision, careless or malicious reporting is possible. Thus, the statute, whether read broadly or narrowly, means that some "wrongs" will go unredressed. But this is neither novel nor decisive: "rights" are regularly limited or defeated by privileges, immunities, and other defenses of many kinds. . . . In truth, all rights are limited by countervailing concerns and interests. The distinction that calls some of these limitations ones on "remedy" is largely a verbal convenience.[47]

In *Center for National Security Studies v. Department of Justice*,[48] the court set the stage for a revision of an existing consent decree concerning NYPD investigative activities which would expand the abilities of the NYPD in investigative and intelligence activities. The court noted that the USA PATRIOT Act had "recognized the important intelligence gathering information at the grass roots level . . ."[49]

At this time, the courts have revealed that they will give substantial deference to executive decisions made pursuant to the USA PATRIOT Act, that they will reject a broad scope of constitutional arguments aimed at the USA PATRIOT Act, that they will seek a constitutional reading of the USA PATRIOT Act, that they will provide very substantial protection to the release of information concerning the activities of the government pursuant to the USA PATRIOT Act for which the government seeks protection, and that those who provide information concerning possible illegal activities to the government will receive very substantial protection from civil liability.

IX. Conclusion

Has the USA PATRIOT Act struck the right balance between the security of the People and the liberty of the People? Do we simply not know whether an arguably unnecessary intrusion upon individual liberties has occurred due to government secrecy? The bottom line is that we the People will need to trust the institutions which have served as so well throughout the existence of the Republic, especially our independent judiciary, and a vigorous and ongoing public debate concerning the balance struck by the USA PATRIOT Act.

44. 18 USC §1993.
45. 320 F.3d 26 (1st Cir. 2003).
46. 31 U.S.C. §5318.
47. 320 F. 3d at 33.
48. 331 F.3d 918 (D.C. Cir. 2003).
49 277 F. Supp. 2d at 341.

Consumer Privacy and Preemption: An Overview of Gramm-Leach-Bliley, The Fair Credit Reporting Act and Proposed 2003 Legislative Amendments

By Virginia N. Roddy

IADC member Virginia N. Roddy is a founding partner of the firm Preaus, Roddy & Associates, LLP in New Orleans. Since her admission to the bar in 1979, she has practiced primarily in the areas of life, health and disability insurance defense litigation. Beginning in the early 1980s, she developed experience as trial and appellate counsel in handling cases involving claims for benefits under plans governed by the Employee Retirement Income Security Act.

I. Introduction

The Gramm-Leach-Bliley Act[1] (GLBA) sets minimum standards for protecting the privacy of consumers' personal financial information.[2] The Fair Credit Reporting Act[3] (FCRA) protects consumers from inaccurate and inappropriate disclosure of their personal information by consumer reporting agencies (CRA),[4] and governs the disclosure of consumer reports.[5] Together, GLBA and FCRA contain the most comprehensive privacy policies ever enacted.[6]

On July 24, 2003, the House Committee on Financial Services overwhelmingly passed H.R. 2622, characterized as "landmark bipartisan legislation," to provide consumers with greater identity theft protection and to amend section 624 of FCRA to remove the January 1, 2004 sunset of the uniform national consumer protection standards and make them permanent.[7] The bill was placed on the House Calendar for con-

1. Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 U.S.C. and 15 U.S.C.) (enacted Nov. 12, 1999) (hereinafter GLBA).

2. The privacy provisions of GLBA are set forth in Subtitle A of Title V; Pub. L. No. 106-102, §§ 501-510, 15 U.S.C. §§ 6801-6809 (2000).

3. In 1970, Congress amended the Consumer Credit Protection Act, 15 U.S.C. § 1601 et seq., by adding a number of provisions collectively known as the Fair Credit Reporting Act (FCRA). Fair Credit Reporting Act, Pub. L. No. 91-508, Title VI, 84 Stat. 1127 (1970) (codified in 15 U.S.C. § 1681, et seq.) (enacted Oct. 26, 1970).

4. The term "consumer reporting agency" is defined as:
[A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.
15 U.S.C. § 1681a(f).

5. *See* 15 U.S.C. § 1681b. "Consumer reports" are defined as: [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living in establishing the consumer's eligibility for - (A) credit or insurance to be used primarily for personal, family or household purposes;
. . .
Id. at § 1681a(d)(1)(A) (emphasis added). A central purpose of FCRA is to ensure the "confidentiality, accuracy, relevancy, and proper utilization of [consumers' credit information]." *Id.* at § 1681. Consumers may bring suit for either willful or negligent violations of FCRA's requirements. *See id.* at §§ 1681n, 1681o (1994 ed.)
Congress enacted the FCRA in 1970 to promote efficiency in the Nation's banking system and to protect consumer privacy. . . . [T]he Act seeks to accomplish those goals by requiring credit reporting agencies to maintain 'reasonable procedures' designed 'to assure maximum possible accuracy of the information' contained in credit reports, and to 'limit the furnishing of [such reports] to' certain statutorily enumerated purposes. The Act creates a private right of action allowing injured consumers to recover 'any actual damages' caused by negligent violations and both actual and punitive damages for willful noncompliance.
TRW, Inc. v. Andrews, 534 U.S. 19, 23 (2001); *see also* Stafford v. Cross County Bank, 2003 WL 21058173 (W.D. Ky. May 8, 2003).

6. See 145 Cong. Rec. H11, 539-40, 544 (daily ed. Nov. 4, 1999). *See also An Examination of Existing Federal Statutes Addressing Information Privacy: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 107th Cong. 20-22 (April 3, 2001), Serial No. 107-22 (statement of L. Richard Fischer, Partner, Morrison and Foerster).

7. House Committee on Financial Services [Committee News], *Committee Approves Landmark Identity Theft Legislation* 61-3 (July 24, 2003), http://financialservices.house.gov/News.asp?FormMode=release&ID=380 (last visited August 22, 2003); *see also* 15 U.S.C. § 1681t(3)(d)(2)(A); H.R. 2622, 108th Cong. (2003); H.R. Rep. No. 108-263 (2003). *See infra* Part IV.1.

sideration[8] and, on September 10, 2003, it passed the House by a vote of 392-30.[9] On September 11, 2003, the bill was referred to the Senate Committee on Banking, Housing and Urban Affairs.[10]

Legislation has also been introduced to amend GLBA by providing stricter privacy protections and requiring affirmative consent from consumers before their information is disclosed (opt-in versus the current opt-out provisions).[11] Competing legislation seeks to retain the current opt-out provisions and amend GLBA by making the privacy provisions preemptive.[12] Unlike FCRA, GLBA does not preempt the states from enacting more stringent privacy regulations.[13]

II. Overview of Title V of Gramm-Leach-Bliley: the Privacy Provision

GLBA repealed the Glass-Steagall Act, thereby eliminating the long-standing prohibition against cross-ownership and affiliation among banks, security brokerage firms, and insurance companies.[14] The purpose of GLBA is "to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers . . . ."[15] Insurance companies, securities firms and banks may now acquire, affiliate with, or engage in any activities that are "financial in nature," including "insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent or broker for purposes of the foregoing in any State."[16]

Recognizing the concerns of consumers regarding the dissemination of private financial information, Congress enacted Title V.[17] Entitled "Privacy," Title V protects consumers[18] and customers[19] from certain disclosures of nonpublic personal information[20] by financial institutions and requires

8. *See* House Calendar, 108th Cong. (Sept. 9, 2003), available at http://frwebgate. access.gpo.gov/cgi-bin/getdoc.cgi ?dbname=house_calendar&docid=f:hc03.pdf (last visited September 10, 2003); *see also* Office of the Clerk, U.S. House of Representatives, Current House Floor Proceedings, at http://clerk.house.gov/floorsummary/floor.php3 (last visited September 10, 2003). The status of the bill can be reviewed at http://thomas.loc.gov/cgi-bin/ bdquery /z?d108:h.r.02622. *See also* H.R. Rep. No. 108-263 (2003).

9. *See* Office of the Clerk, U.S. House of Representatives, Current House Floor Proceedings, at http://clerk.house.gov/ floorsummary/floor.php3 (last visited September 10, 2003).

10. *See* http://thomas.loc.gov/cgi-bin/ bdquery/z?d108: h.r.02622.

11. *See infra* Part IV.

12. *See id.*; *see also* H.R. 1766, 108th Cong. (2003); infra Part IV.2.

13. *See* 15 U.S.C. § 6807; *infra* Part II.

14. *See* 12 U.S.C. § 377(a); Pub. L. No. 106-102, Title I, § 101.

15. H.R. Conf. Rep. No. 106-434, at 245 (1999), *reprinted in* 1999 U.S.C.C.A.N. 245, 245.

16. 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k)(4)(B), Pub. L. No. 106-102, Title I, § 103. Therefore, under GLBA, insurance companies qualify as financial institutions. *See id.*; *see also infra* notes 43-44 and accompanying text.

17. *See* H.R. Rep. 106-74, pt.3, at 106-07 (1999) ("As a result of the explosion of information available via electronic services such as the Internet, as well as the expansion of financial institutions through affiliations and other means as they seek to provide more and better products to consumers, the privacy of data about personal financial information has become an increasingly significant concern of consumers.") Title V of GLBA includes the statement that, "It is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. For a discussion of the legislative history of GLBA and issues relating to whether promulgation of regulations under GLBA contravened the plain meaning of GLBA and violated credit reporting agencies' rights to equal protection, due process and free speech under the First Amendment, see Individual Reference Services Group v. Federal Trade Commission, 145 F.Supp.2d 6 (D.D.C. 2001); Trans Union LLC v. Federal Trade Commission, 295 F.3d 42 (D.C. Cir. 2002).

18. "Consumer" is defined as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family or household purposes[.]" 15 U.S.C. § 6809(9).

19. A "customer" is a consumer with whom a "customer relationship" has been established with a financial institution. 15 U.S.C. § 6809(11); *see also* 15 U.S.C. § 6803(a). Under GLBA, both consumers and customers are given opt-out rights. *See* 15 U.S.C. § 6802.

20. The term 'nonpublic personal information' means personally identifiable financial information -
(i) provided by a consumer to a financial institution;
(ii) resulting from any transaction with the consumer or any service performed for the consumer; or
(iii) otherwise obtained by the financial institution.
(B) Such term does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of this title.
(C) Notwithstanding subparagraph (B), such term -
(i) shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but
(ii) shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. 15 U.S.C. § 6809(4)(A)(B)(C).

financial institutions[21] to protect the privacy of consumers by:

- developing, creating and maintaining privacy policies and disclosing these privacy policies to its customers and consumers[22]
- giving customers and consumers, in certain circumstances, the right to opt-out of information sharing with nonaffiliated third parties before their nonpublic personal information is disclosed[23]

Under Title V, privacy notices must be given to customers at the inception of the customer relationship with the financial institution and not less than annually thereafter.[24] The privacy notices inform customers of the financial institutions' privacy policies, including how and where the institution obtains private customer information, how this information can be used and to whom it may be disclosed.[25]

The "opt-out" provision contained in Title V is limited, in that GLBA only allows a consumer to opt-out of the disclosure of his nonpublic personal information to nonaffiliated third parties with whom the institution does not have a joint marketing agreement.[26] GLBA does not permit a consumer to opt-out of information sharing among affiliated companies[27] or among nonaffiliated third parties who have a "joint marketing" arrangement.[28] However, a financial institution "shall not disclose, other than to a consumer reporting agency," a consumer's account number or other similar access code "for a credit card account, deposit account, or transaction account . . . to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer."[29]

There are a number of statutory exceptions under Title V, which permit disclosure of a consumer's nonpublic personal information in certain circumstances.[30] These include disclosures as necessary to handle a transaction, service, or financial product requested by the consumer, maintaining or servicing the consumer's account, and disclosures that are with the consent or at the direction of the consumer.[31] Furthermore, disclosures may be made to protect the confidentiality and security of the financial institutions' records pertaining to the consumer, to protect against fraud, to consumer reporting agencies, in connection with the sale, merger, or transfer of business, to comply with subpoena or summons by a federal, state, or administrative authority, to comply with federal, state, or local rules, or to the extent otherwise specifically permitted by law.[32]

Enforcement of GLBA is by the regulatory agency or authority with jurisdiction over the financial institution.[33] Title V specifically designates the Department of Insurance as the agency to establish the appropriate standards covering any person engaged in providing insurance under state law. It states: "This subtitle and the regulations prescribed thereunder shall be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons sub-

21. "Financial institutions" are defined as "any institution the business of which is engaging in financial activities described in section 4(k) of the Bank Holding Act of 1956." 15 U.S.C. § 6809(3)(A); s*ee supra* note 16 and accompanying text.

22. *See* 15 U.S.C. § 6803.

23. *See id*. at § 6802.

24. *See id.* at § 6803(a). Privacy notices must be given to consumers at the time of their transaction with the financial institution. *See id.* at § 6802(a).

25. *See id.* at § 6803(b).

26. *Id*. at § 6802(b)(1).

27. *See id.* at § 6802. "Affiliate" means any company that controls, is controlled by, or is under common control with another company. *Id.* at § 6809(6).

28. 15 U.S.C. § 6802(b)(2). A financial institution may disclose nonpublic personal information to a nonaffiliated third party for the purposes of "perform[ing] services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services," if the financial institution fully discloses the providing of such information and the third party enters into an agreement to maintain the confidentiality of the information. *Id.* A nonaffiliated third party who receives nonpublic personal information may not disclose it to any other nonaffiliated third party, unless disclosure would be lawful if made directly by the financial institution to the other person. *See id.* at (c).

29. *Id.* at § 6802(d).

30. *See id.* at § 6802(e).

31. *See id.* at (e)(i)(2).

32. *See id.* at (e)(3)-(8).

33. *See* 15 U.S.C. § 6805; *see also* 15 U.S.C. § 6801(b).

ject to their jurisdiction under applicable law."[34] Under state insurance law, enforcement of GLBA is by the applicable state insurance authority.[35] The regulators are also responsible for establishing "appropriate standards for the financial institutions ...relating to administrative, technical, and physical safeguards:"

(1) to ensure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[36]

GLBA does not grant an express private right of action to enforce its provisions or to seek redress for violations of the Act.[37] Some courts, however, have found that an implied private right of action exists.[38]

As noted earlier, unlike FCRA, GLBA does not preempt state laws, except to the extent that the state law is inconsistent with a provision of Title V, and then only to the extent of the inconsistency.[39] However, "a State statute, regulation, order or interpretation is **not** inconsistent with the provisions of [Title V] if the protection such statute, regulation, order or interpretation affords any person is **greater** than the protection provided under [Title V]."[40]

III. The FCRA

FCRA excludes from the definition of "consumer reports" consumer information that is shared by corporate affiliates.[41] It also contains certain preemption provisions, including the prohibition of state laws that regulate the sharing of consumer information among affiliates.[42]

FCRA allows a consumer reporting agency to furnish a consumer credit report "[t]o a person which it has reason to believe . . . intends to use the information in connection with the underwriting of insurance involving the consumer."[43] Insurance companies may therefore be held liable under FCRA if they fail to insure the "confidentiality, accuracy, relevancy, and proper utilization" of a consumer's credit information.[44]

The Federal Trade Commission (FTC), as the agency authorized with administering the FCRA,[45] has defined "underwriting of insurance" as follows: "An insurer may obtain a consumer report to decide whether or not to issue a policy to the consumer, the amount and terms of the coverage, the duration of the policy, the rates or fees charged, or whether or not to renew or cancel a policy, because these are all 'underwriting' decisions."[46]

IV. Proposed Legislation Amending FCRA and GLBA

A number of bills were introduced during the 2003 legislative session to amend FCRA and GLBA. Among them are the following:

1. Fair and Accurate Credit Transactions Act (FACT)

As mentioned above, on September 10, 2003, the House passed legislation that would make permanent certain preemption provisions of FCRA.[47] H.R. 2622, known

34. 15 U.S.C. § 6805(a). GLBA expressly states that the McCarran-Ferguson Act, 15 U.S.C. §§ 1011-1015, "remains the law of the United States." 15 U.S.C. § 6701(a). The McCarran-Ferguson Act ensures that the states bear the primary responsibility of regulating insurance. *See* 15 U.S.C. § 1012.

35. *See* 15 U.S.C. § 6805(a)(6).

36. *Id.* at § 6801(b).

37. *See* 15 U.S.C. § 6801, *et seq*.

38. *See infra* Part VI.

39. *See* 15 U.S.C. § 6807(a)

40. *Id.* at § 6807(b) (emphasis added).

41. 15 U.S.C. § 1681a(d)2)(A)(ii).

42. *See id.* at § 1681t(2); see supra note 5.

43. *Id.* at § 1681b(a)(3)(C).

44. *See* St. Paul Guardian Ins. Co. v. Johnson, 884 F.2d 881, 883 (5th Cir. 1989).

45. *See* 15 U.S.C. § 1681s(a).

46. FTC Commentary on the Fair Credit Reporting Act, 16 C.F.R. pt. 600, App. *See also* Scharpf v. AIG Marketing, Inc., 242 F.Supp.2d 455, 462 (W.D. Ky. 2003) ("In effect, the FCRA created a fair mechanism through which creditors and insurers could obtain a consumer's report in order to make an offer [of credit or insurance] and evaluate creditworthiness").

47. H.R. 2622, 108th Cong. (2003) (Sponsored by House Financial Institutions Subcommittee Chairman Spencer Bachus (R-AL)). *See supra* notes 7-9 and accompanying text. If signed into law, the preemption provisions of FCRA will become permanent. *See* H.R. 2622, at Title I, § 101.

as the Fair and Accurate Credit Transactions Act (FACT) also includes a number of provisions relating to identify theft and fraud, improving the accuracy of consumer credit information, and granting consumers the right to request one free credit report each year.[48] Under FACT, CRAs would be required to place a "fraud alert" in a consumer's file if the consumer believes that he is, or is about to become, a victim of identity theft.[49]

2. National Uniform Privacy Standards Act of 2003

Introduced on April 11, 2003 by Rep. Patrick J. Tiberi (R-OH), the National Uniform Privacy Standards Act of 2003 makes permanent the preemption provisions of FCRA and amends GLBA by preempting states from enacting any requirement or prohibition with respect to any subject matter regulated by GLBA.[50] The bill establishes a uniform national privacy standard for financial institutions by prohibiting states from enacting "opt-in" privacy requirements or more strict privacy laws than those currently under FCRA and GLBA.[51]

3. Identity Theft Consumer Notification Act

The Identity Theft Consumer Notification Act, introduced by Rep. Gerald D. Kleczka (D-WI) on February 13, 2003, amends GLBA by requiring financial institutions to notify consumers if their private financial information has been compromised and to reimburse consumers for any resulting damages.[52] It also amends FCRA by establishing a private right of action to enforce "any liability created under this title."[53]

4. Privacy Act of 2003

On March 31, 2003, Senator Diane Feinstein (D-CA) introduced the Privacy Act of 2003, which amends GLBA by prohibiting the disclosure of personal financial information by commercial entities to nonaffiliated third parties unless the consumer first consents, or opts-in, to the disclosure.[54] It also prohibits entities from sharing information among affiliates and nonaffiliated third parties under a joint marketing agreement unless consumers are first given a right to opt-out of such disclosures.[55] Additional prohibitions exist for the disclosure of social security numbers, drivers license data, and health information.[56]

5. Privacy Protection Clarification Act - Exempting Lawyers from the Disclosure Requirements of GLBA

On February 13, 2003, Rep. Judy Biggert (R-IL) introduced the Privacy Protection Clarification Act to exempt lawyers from the privacy provisions of GLBA.[57] Financial institutions must comply with the privacy, disclosure and notice provisions of GLBA.[58] Under the bill, an amendment to GLBA explicitly excludes lawyers from the definition of "financial institution," which currently contains no reference to law firms or lawyers.[59]

Concerned that attorneys might be considered by the FTC as "financial institu-

48. *See id*. at Title II, IV, V.

49. *Id.* at Title II, § 202. A "fraud alert" is a "clear and conspicuous statement in the file of a consumer that notifies all prospective users of a credit report . . . that the consumer does not authorize the issuance or extension of credit in the name of the consumer." *Id.* Unless it receives express permission from the consumer, an issuer or extender of credit cannot issue or extend credit in the name of the consumer. *See id.* Additionally, CRAs must notify each person who procures a credit report of the fraud alert. *See id.*

50. H.R. 1766, 108th Cong. (2003), § 3.

51. *See* H.R. 1766. No action has been taken on H.R. 1766 since it was referred to the House Subcommittee on Financial Institutions and Consumer Credit on April 29, 2003. *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.01766: (last visited September 10, 2003).

52. H.R. 818, 108th Cong. (2003).

53. *Id.* No action has been taken on H.R. 818 since it was referred to the House Subcommittee on Financial Institutions and Consumer Credit on February 27, 2003. *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.00818: (last visited September 10, 2003).

54. S. 745, 108th Cong. (2003), Title III, § 302.

55. *See id.*

56. *See* S. 745, Title II, IV, V. S. 745 was referred to the Senate Committee on the Judiciary March 21, 2003. No action has been taken since that date. *See* http://thomas.loc.gov/ cgi-bin/bdquery/z?d108:s.0745: (last visited September 10, 2003).

57. H.R. 781, 108th Cong. (2003).

58. *See* 15 U.S.C. § 6801, *et seq.*

59. *See* 15 U.S.C. 6809(3); H.R. 781. No action has been taken on H.R. 781 since it was referred to the House Subcommittee on Financial Institutions and Consumer Credit on March 10, 2003. *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.00781: (last visited September 10, 2003).

tions" and thereby subject to GLBA's disclosure requirements,[60] the American Bar Association (ABA) and the New York State Bar Association (NYSBA), in separate suits, brought actions against the FTC, seeking a ruling that lawyers are not financial institutions and therefore exempt from the privacy provisions of GLBA.[61] The FTC filed motions to dismiss both actions, which were heard by Judge Reggie Walton of the United States District Court, District of Columbia.[62]

On August 11, 2003, in denying the FTC's motions to dismiss, Judge Walton issued a preliminary ruling that the FTC may have acted beyond its authority and engaged in "arbitrary and capricious" conduct when it determined that lawyers were covered by the privacy notification provisions of GLBA.[63] Judge Walton stated, "It does not appear that Congress intended for the privacy provisions of the GLBA to apply to attorneys."[64] The case will likely proceed on summary judgment.[65]

V. The National Association of Insurance Commissioners (NAIC) Rules and Regulations and State Laws Implementing GLBA

Since the 1980s, the National Association of Insurance Commissioners (NAIC) has adopted model acts and regulations concerning the privacy of insurance consumer's personal information, including the Insurance Information and Privacy Protection Model Act of 1982 ("1982 Model Act"),[66] the Privacy of Consumer Financial and Health Information Model Regulation of 2000 ("2000 Model Regulation"),[67] and Standards for Safeguarding Customer Information Model Regulation in April 2002 ("Safeguarding Standards").[68]

All 50 states and the District of Columbia have taken steps to put privacy protections in place by either adopting new laws or amending existing laws to comply with GLBA standards.[69] Fourteen states

60. GLBA requires certain federal agencies, including the FTC, to issue final rules necessary to carry out the purposes of Subtitle A of Title V. *See* 15 U.S.C. § 6804(a)(1). On May 24, 2000, the FTC issued a Final Rule, which did not specifically exempt lawyers from the privacy provisions of GLBA. *See* 16 C.F.R. § 313.18; *see also* Center for Regulatory Effectiveness, *FTC Determines Attorneys to be Subject to Notice Requirements of Gramm-Leach-Bliley Act* (reprinting letter from the Boston Bar Association to the FTC (Feb. 23, 2001), available at http://www.thecre.com/emerging/) ("The Federal Trade Commission (FTC) has determined that law firms must comply with the notice provisions included in the 1999 Gramm-Leach-Bliley financial modernization legislation. According to the FTC, attorneys may provide "financial services" under the Act, thereby triggering the notice provisions related to the privacy of consumer financial information.")

61. New York State Bar Ass'n v. Federal Trade Comm'n, 2003 WL 21919841 (D.D.C. Aug. 11, 2003). More than a dozen state bar associations and the Conference of Chief Justices filed amicus briefs siding with the ABA and NYSBA. *See id.* at *30, n.8. The suits filed by the NYSBA and the ABA were consolidated.

62. New York State Bar Ass'n v. Federal Trade Comm'n, 2003 WL 21919841. In a letter dated June 30, 2003, counsel for the FTC informed counsel for the ABA and NYSBA that the FTC does "not intend to bring any enforcement actions under [GLBA provisions 15 U.S.C. §§ 6801-6809] against lawyers for any action or inaction by lawyers in the period of time prior to the Court's rulings on the FTC's motions to dismiss [the cases brought by ABA and NYSBA]." *Id.* at *30, n.1.; *see also* Letter from William E. Kovacie, General Counsel, Federal Trade Commission, to David L. Roll, Esq., counsel for the American Bar Association, and Warren L. Dennis, Esq., counsel for the New York State Bar Association (June 30, 2003), available at http://www.abanet.org/poladv/glbfactsheet/ amnestyletter.pdf.

63. See id. at *24-25, 30.

64. *Id.* at *11, 30. Stating that attorneys were not "financial institutions," Judge Walton also noted that state law regulates lawyers and the practice of law, not the federal government. *Id.* at *6, 12, 14.

65. *See id*. at *30, n.26.

66. Insurance Information and Privacy Protection *Model Act, Model Laws, Regulations and Guidelines*, NAIC Model V-670, available at http://www.naic.org/library/ reference/subjects/privacy.htm (last visited August 25, 2003).

67. *Privacy of Consumer Financial and Health Information Regulation, Model Laws*, Regulations and Guidelines, NAIC Model IV-672, available at http://www.naic.org/ library/reference/subjects/privacy.htm (last visited August 25, 2003).

68. Standards for Safeguarding Consumer Information *Model Regulation, Model Laws, Regulations and Guidelines*, NAIC Model IV-673, available at http://www.naic.org/library /reference/subjects/privacy.htm (last visited August 25, 2003).

69. See RICHARD J. HILLMAN, FINANCIAL PRIVACY: STATUS OF STATE ACTIONS ON GRAMM-LEACH-BLILEY ACT'S PRIVACY PROVISIONS, Gen. Accounting Office 02-361, p. 6 (April 12, 2002).

Some municipal governments have also adopted ordinances or regulations to provide greater consumer protection than that afforded under GLBA. For example, the San Francisco Financial Information Privacy Ordinance, effective January 21, 2004, requires financial institutions to first obtain the consent of San Francisco customers before the disclosure or sharing of private information to affiliates or nonaffiliated third parties. San Francisco, Cal., Financial Information Privacy Ordinance 237-02, § 2004 (Dec. 20, 2002), available at http://www.amlegal.com/nxt/gateway.dll?f=templates&fn=default.htm&vid=alp:sf_business (last visited August 25, 2003). The ordinance "afford[s] consumers greater privacy protection than that provided in [Gramm-Leach-Bliley]." *Id.* at § 2001(b). It also imposes penalties for the negligent and wilful disclosure of confidential consumer information in violation of the

have laws based on the 1982 Model Act[70] and 35 states plus the District of Columbia have issued regulations based on the 2000 Model Regulation.[71] NAIC members adopted the 2000 Model Regulation "to facilitate a uniform state approach to implementing the disclosure-related requirements of Subtitle A [of Title V of GLBA]."[72] The Safeguarding Standards, which were established to provide model standards for insurers to meet the confidentiality and security requirements of section 501 of GLBA, has not been widely adopted by the states.[73]

VI. Privacy Litigation Under GLBA

Title V of GLBA does not contain an express private right of action provision that would enable consumers to bring suit for violations of GLBA's requirements or to enforce its provisions.[74] Enforcement is left to the federal agencies and the state insurance agencies that have jurisdiction over financial institutions covered by the rule.[75]

In *Conboy v. AT & T Corp.*,[76] a consumer brought suit against AT & T for violations of the Fair Debt Collection Practices Act and Telecommunications Act.[77] The Second Circuit Court of Appeals agreed with the district court in its ruling that the Telecommunications Act did not explicitly or implicitly provide for a private right of action.[78] The Second Circuit stated, "The question of the existence of a statutory cause of action is, of course, one of statutory construction. In this case, the text of the Telecommunications Act contains no language that explicitly provides a private right of action for damages for violations of the two FCC regulations at issue here[79] . . . . Moreover, no private right of action for money damages can be implied."[80]

In analyzing whether a consumer has a private right of action, the Second Circuit Court of Appeals referred to *Cort v. Ash*,[81] in which the Supreme Court established a

ordinance. *See id.* at § 2008.

Vermont and New Mexico have also adopted "opt-in" provisions. *See* VT Reg. IH-2001-01 (no longer available online); N.M. Reg. 13.1.3, at .11, .12 (2002). "This rule governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the NMPRC Insurance Division and is intended to afford individuals greater privacy protections than those provided in the Gramm-Leach-Bliley Financial Modernization Act . . . ." *Id.* at 13.1.3.6.

For a chart of state statutes and regulations relating to GLBA and consumer privacy with respect to insurers, see http://www.llgm.com/articles/article_15_print.asp (last visited September 8, 2003).

70. *See* HILLMAN, *supra* at pp. 9-11; *see also, e.g.*, NEW JERSEY INSURANCE BULLETINS, *Enforcement of Gramm-Leach-Bliley Privacy Requirements*, Bulletin 2000-15 (Nov. 8, 2000), available at http://www.njdobi.org/blt00_15.htm (last visited September 9, 2003) ("N.J.S.A. 17:23A-1 et seq., effective December 7, 1985, and based on the National Association of Insurance Commissioners' Insurance Information and Privacy Protection Model Act, regulates the collection, use and disclosure of information gathered by insurers in connection with policies, contracts or certificates of insurance issued or delivered in this State. In most respects, this statute provides standards that are at least as stringent, and in many cases more stringent, than the standards set forth in GLBA").

71. *See* HILLMAN, *supra* at pp. 6-8.

72. *See id*. at p. 6.

73. *See id.* at pp. 12-13. *See also Summary Of NAIC Fall 2002 Meeting*, http://www.aba.com/NR/ rdonlyres /00006946 qqocodkcytxufioi/NAIC+Fall+2002 +Meeting6.doc (last visited August 22, 2003); *Implementing Privacy Protections*, http://www.naic.org/GLBA/privacy.htm (last visited September 8, 2003).

74. *See* 15 U.S.C. § 6801, *et seq.* The Supreme Court has held that "[t]he question whether Congress . . . intended to create a private right of action [is] definitively answered in the negative" where "a statute by its terms grants no private rights to any identifiable class." Touche Ross & Co. v. Redington, 442 U.S. 560, 576 (1979). The Supreme Court has also held that, for a statute to create private rights of action, its text must be "phrased in terms of the persons benefitted," Cannon v. University of Chicago, 441 U.S. 677, 692, n.13 (1979) and "with an unmistakable focus on the benefitted class." *Id.* at 691. A plaintiff suing under an **implied** right of action must show that the statute manifests an intent "to create not just a private **right**, but also a private **remedy**." Alexander v. Sandoval, 532 U.S. 275, 286 (2001) (emphasis added). *See* Gonzaga University v. Doe, 536 U.S. 273 (2002) (examining private rights of action under 42 U.S.C. § 1983).

75. *See* 15 U.S.C. § 6805. *See supra*, notes 33-35 and accompanying text. For a discussion of consumer privacy litigation related to financial services companies, the internet and other industries during the years 1999 and 2000, see Stephen F. Ambrose, Jr. & Joseph W. Gelb, Consumer Privacy Regulation and Litigation, THE BUSINESS LAWYER, May 2001, http://www.weil.com/wgm/cbyline.nsf/0/a90b82c4728b100a85256a7a00652e5f?OpenDocument. *See also* Ronald L. Plesser & Stuart P. Ingis, Limiting Private Rights of Action In Privacy Legislation, http://www.cdt.org/privacy/ccp/privaterightofaction1.shtml (last visited September 9, 2003) ("As policymakers consider the merits of additional privacy legislation, the potential for abuse that can result from a private right of action must be considered. Statutory damages should not be included in legislation. Where effective government enforcement is available, such enforcement is better policy as it protects consumers and limits frivolous lawsuits.").

76. 241 F.3d 242 (2d Cir. 2001).

77. *See id.* at 246.

78. *See id.* at 252.

79. The two Federal Communications Commission (FCC) regulations referred to in the opinion are 47 C.F.R. §§ 51.217, 64.1201.

80. Conboy, 241 F.3d at 252.

81. 422 U.S. 66 (1975).

four-factor test to determine whether a federal statute creates an implied private right of action:

> (1) whether the plaintiff is one for whose benefit the statute was enacted; (2) whether there is evidence of legislative intent, explic it or implicit, to create or deny a private remedy; (3) whether the existence of a private right of action would be consistent with the underlying legislative purpose of the statute; and (4) whether the cause of action is in an area traditionally left to state law.[82]

Since *Cort*, the Supreme Court has refined this inquiry.[83] The analysis has been simplified to the following inquiry: whether Congress, expressly or by implication, intended to create a private right of action.[84] The Second Circuit in *Conboy* determined that "it is highly unlikely, therefore, that Congress intended to create a private right of action for violations of FCC regulations. Such a right would 'threaten[ ] the sound development of a coherent nationwide communications policy - a central objective of the [Communications] Act."[85]

Since Title V of GLBA was designed to protect the privacy of consumers but does not preempt state laws, it is arguable that it establishes a "coherent nationwide" policy.[86] The Fifth Circuit Court of Appeal is currently considering whether an **implied** private right of action exists under GLBA.

Union Planters Bank, N.A. v. Gavel [Gavel # 1]

In *Union Planters Bank, N.A. v. Gavel*[88] *[Gavel #1]*, Union Planters Bank brought an action in federal court to enjoin the disclosure of private consumer financial information without the prior consent of its customers in violation of GLBA.[89] Gavel, an insurance broker, worked with a company that provided insurance services to Union Planters.[90] In connection with that working relationship, Gavel received information relative to Union Planters customers, which information was sought by way of subpoena in connection with an insurance fraud case filed in state court.[91]

Union Planters sought an injunction from the District Court for the Eastern District of Louisiana, contending that, unless Gavel was enjoined from producing the nonpublic personal information, a clear violation of GLBA would occur.[92] Intervenors moved to dismiss the injunction action on the grounds of res judicata and abstention.[93]

Union Planters alleged that it would suffer irreparable injury to its business reputation when its customers learned that their nonpublic personal financial information had been disclosed to third parties without their prior knowledge or consent.[94] It also alleged that it would be subject to regulatory sanctions for violating GLBA and that an injunction would not be contrary to public interest since GLBA promotes the public interest by protecting the privacy interests of consumers.[95]

The District Court granted the injunction.[96] It found that the information which Gavel had been subpoenaed to produce was

82. *Id.* at 78.

83. *See* Miller v. United States, 710 F.2d 656, 667 (10th Cir. 1983), *cert. denied*, 464 U.S. 939 (1983).

84. *See* Transamerica Mortgage Advisors, Inc. v. Lewis, 444 U.S. 11, 15-16 (1979); Touche Ross & Co. v. Redington, 442 U.S. 560, 575 (1979); *see also* Thompson v. Thompson, 484 U.S. 174, 189 (1988) (Scalia, J., concurring) ("[W]e effectively overruled the Cort v. Ash analysis in Touche Ross [and Transamerica], converting one of its four factors (congressional intent) into the determinative factor."). The other Cort factors are relevant insofar as they assist in determining congressional intent. *See* Touche Ross, 442 U.S. at 575-76.

85. *Conboy*, 241 F.3d at 253, quoting New England Tel. & Tel. Co. v. Public Utils. Comm'n, 742 F.2d 1, 6 (1st Cir. 1984). The Second Circuit noted that, while plaintiffs did not have a private right of action under the Telecommunications Act, they could have sought relief by filing a complaint with the FCC. *See id*. at 256. The FCC, as the regulatory authority under the Telecommunications Act, could have investigated the claim of plaintiffs and imposed penalties as permitted under the statute. *See id.* "Plaintiffs therefore had a forum in which to complain about the behavior alleged in their amended complaint, and to obtain relief if appropriate; however, they chose to seek relief elsewhere." *Id.*

86. *Id*. at 253; 15 U.S.C. §§ 6801, 6807.

87. *See infra* note 104.

88. 2002 WL 975675 (E.D. La. May 9, 2002), reconsideration denied 2002 WL 1379182.

89. *See id.* at *1.

90. *See id.* at *5.

91. *See id.*

92. *See id.* at *2.

93. *See id.*

94. *See id.*

95. *See id.*

96. *See id.* at *6.

nonpublic personal financial information, the disclosure of which was prohibited by GLBA.[97] It further found that irreparable injury would result since, once the information was disclosed, no monetary relief could be awarded to compensate for the loss and Union Planters could suffer "grave consequences" if the information were disclosed.[98] The Court concluded that "the injunction in no way would disserve the public interest as the injunction would merely uphold and enforce a federal statute."[99] The opinion did not address whether Union Planters had a private right of action under GLBA.

Union Planters v. Gavel [Gavel # 2]

On March 12, 2003, in *Union Planters v. Gavel*[100] *[Gavel #2]*, the District Court for the Eastern District of Louisiana granted Union Planters' motion to make the preliminary injunction granted in *Gavel #1* permanent.[101] In *Gavel #2*, the intervenors argued that, since the injunction was premised on GLBA, Union Planters had no right of action or standing to bring an action because GLBA does not grant a private right of action to enforce the provisions of GLBA.[102]

In granting Union Planters request for a permanent injunction, the District Court stated:

> The GLBA is written with the protection of the customers of the financial institutions in mind. . . . The subpoena issued in the state court proceeding seeks full disclosure of the very nonpublic consumer information which GLBA seeks to protect. . . . Since the subpoena seeks disclosure of information which otherwise would, by law, remain confidential, the action by Plaintiff to seek injunctive relief as to the specific nonpublic consumer information is correct. . . . The purpose of the injunction is to stop the release of that information before it is made public. The Plaintiff has a definite right of action in that this injunction seeks to protect the Plaintiff's information. . . . The subpoena asks that this information be yanked out from the cloak of the protection . . . of the . . GLBA. The Court has twice ruled that the Intervenor should be enjoined from gaining access to the nonpublic consumer information, and today, the Court maintains its previous reasoning.[103]

The case has been appealed to the U.S. Fifth Circuit Court of Appeal.[104] Appellant's Brief was filed on September 11, 2003.[105]

New York Life Insurance and Annuity Corporation v. Filo

While the District Court for the Eastern District of Louisiana found that Union Planters had a private right of action to request an injunction prohibiting disclosure of nonpublic information protected by GLBA, in *New York Life v. Filo*, the District Court for the Western District Court of Louisiana held otherwise.[106] The facts of *Gavel* and *Filo* are similar; the results are different.

In December 2002, New York Life Insurance Company (New York Life) filed a Complaint for injunctive relief and for a temporary restraining order in the United

---

97. *See id.* at *5-6. The District Court recognized that GLBA prohibits the disclosure of nonpublic personal financial information to third parties unless the consumer is given an opportunity, prior to the disclosure, to direct that the information not be disclosed. *See id.* at *5. Cf. Landry v. Union Planters Corp., 2003 WL 21355462, at *5-6 (E.D. La. June 6, 2003) (ordering the disclosure of "blind" documentation, in which personal identifiers had been redacted, in ruling on a motion to quash depositions and requests for production of documents, but ordering the issuance of a protective order, "given the confidential nature of even the redacted discovery"). All federal district courts now require redaction of personal identifiers in documents filed into the record. *See* Judiciary Privacy Policy page, at http://www.privacy. uscourts.gov/ (last visited October 10, 2003).

98. *Gavel*, 2002 WL 975675, at *5.

99. *Id.*

100. 2003 WL 1193671 (E.D. La. March 12, 2003).

101. *See id.* at *9.

102. *See id.* at *3.

103. *Id.* at *9 (emphasis added).

104. Union Planters v. Gavel, No. 03-30409 (5th Cir. (La.)), at http://www.ca5. uscourts.gov/Opinions/pacer.cfm

105. *See* Union Planters v. Gavel, No. 03-30409 (5th Cir. (La.)), at http://www.ca5. uscourts.gov/Opinions/pacer.cfm. Appellants brief, originally due August 27, 2003, is now due September 11, 2003. *See id.*

106. New York Life Insurance and Annuity Corporation v. Filo, No. CV02-2556 (W.D. La. May 21, 2003) (hereinafter New York Life v. Filo). The Complaint, Motions to Dismiss, Memoranda in Support and in Opposition, and the Court's Ruling are all available on PACER, at http://pacer.lawd.uscourts.gov.

States District Court for the Western District of Louisiana, seeking an order prohibiting the disclosure by New York Life of its customers' personally identifiable financial information protected under GLBA without the customers' knowledge and consent.[107] The defendants, Thomas Filo, an attorney, and Steven Blount, a former insurance agent with New York Life, moved to dismiss the Complaint on the basis that GLBA did not create a private right of action.[108]

In its Complaint, New York Life alleged that Filo, an attorney who represented certain New York Life customers in actions brought by New York Life customers against Blount for fraudulent insurance practices, made numerous attempts to obtain a list of and information about customers who were not his clients.[109] Like the intervenors in *Union Planters v. Gavel*, Filo had sought nonpublic information through discovery propounded in a state court proceeding. New York Life had moved to quash the subpoena and sought a protective order on the basis that the information sought was "tantamount to a customer list," which New York Life argued was protected from disclosure under GLBA.[110] The state court judge granted New York Life's motion to quash, ordering that Filo was not entitled to a customer list.[111]

In the federal court proceeding, New York Life alleged that, despite the state court's ruling, Filo continued to obtain and disseminate nonpublic personal information of its customers and that Filo sent hundreds of "advertisements" to those customers in an effort to develop more clients.[112] Customers of New York Life allegedly called New York Life to inquire as to how Filo had obtained their name and address.[113]

In arguing to the federal court that injunctive relief was appropriate, New York Life, conceding that GLBA does not grant a private right of action, stated: "New York Life is without adequate remedy at law to protect its rights and those of its customers, which New York Life is required by law to protect. New York Life has **no private right of action** under state or federal privacy laws to redress the unlawful disclosure of confidential consumer information."[114] New York Life cited to *Union Planters v. Gavel* in support of its argument that an injunction should be entered.

Notwithstanding the decisions in *Gavel #1* and *Gavel #2*, the district court in *Filo* granted defendants' Motions to Dismiss.[116] In its Ruling dated May 21, 2003, the Court stated:

> The Court finds that **New York Life cannot state a cause of action under the GLBA** or Regulation 76 because those enactments **do not provide for private suits to enforce their terms**. The plain language of the GLBA grants federal and state regulatory agencies exclusive authority to prosecute violations of the GLBA and to enforce its provisions. Neither Congress nor the Louisiana legislature extended enforcement of the GLBA or Regulation 76 beyond the administrative action of specified federal or state regulators.[117]

At the time of the writing of this Article, the Fifth Circuit had not ruled on the issues in *Gavel*.[118] The *New York v. Filo* case was closed May 22, 2003 and the decision was not appealed.[119]

VII. Conclusion

In the event that pending legislation is enacted into law, insurers and other financial institutions may be required to revise their disclosure policies. GLBA's effect on the business of insurance and other financial institutions has been significant and will continue to be. Judicial interpretations of GLBA are inconsistent and should be of interest to all companies subject to its provisions.

---

107. *See id.*, Complaint.
108. *See id.*, Motions to Dismiss filed by Filo and Blount.
109. *See id.*, Complaint, at 8.
110. *Id.*, Complaint, 9, 13. In Union Planters v. Gavel, the District Court for the Eastern District of Louisiana noted that the records sought by plaintiffs regarding Union Planters' customers "constitutes a 'grouping' of non-public personally identifiable financial information which is precluded by the GLBA." 2002 WL 975675, at *6.
111. *See* New York v. Filo, Complaint, at 14.
112. *Id.* at 19.
113. *See id.*
114. *Id.*, Complaint, at 28 (emphasis added).
115. *See id.*, Opposition to Defendant's Motion to Dismiss, at 13-14, 16.
116. *See id.*, Ruling, at 6.
117. *Id.*, at 4-5 (emphasis added).
118. *See supra* notes 104-05.
119. *See* New York Life v. Filo, No. 02-CV-2556 at http://pacer.lawd.uscourts.gov.

The Privacy Project II

Protection Against Discovery in Civil and Criminal Proceedings in Clergy Sexual Abuse Claims

By Ralph M. Streza and L. Gino Marchetti, Jr.

In recent years, allegations of sexual abuse by priests have spread from a few relatively isolated instances to a crisis of national and international proportions. In addition to the emotional and psychological (not to mention public relations) issues presented by these cases, counsel retained to defend the diocese, parish or religious institution which employed the offending cleric is presented with complex constitutional issues which must be applied judiciously to be effective in the evaluation and defense of these claims.

Added to the problems of defending the merits of these claims are the procedural and discovery related issues presented by competent plaintiff's counsel who often collaborate with other counsel who specialize in molestation cases as well as with prosecuting attorneys pursuing the offending cleric in the criminal arena.

Certain Constitutional prohibitions can be applied in the discovery process. Indeed, perhaps the most basic form of protection against document discovery may be provided by noting at the outset that certain subject matters cannot be decided by civil courts due to these constitutional prohibitions.

I. Actions Taken By a Religious Entity Are Constitutionally Protected By the First and Fourteenth Amendments of the United States Constitution

The religious freedom clauses of the First Amendment, as applied to the States through the Fourteenth Amendment, provide that: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof . . . ."[1] U.S. Const. Amend. I. The First Amendment's "wall of separation" between Church and State remains "high and impregnable." *McClure II*.[2] 460 F.2d at 558. For well over 100 years courts have applied First Amendment principles in limiting the role of civil courts in resolving religious controversies that incidentally affect civil rights and remedies of individuals.[3] *See, e.g., Watson v. Jones*, 80 U.S. (13 Wall.) 679 (1872); *Presbyterian Church v. Hull Church*, 393 U.S. 440 (1969); *Serbian Eastern Orthodox Diocese v. Milivojevich*, 426 U.S. 696 (1976).

IADC member Ralph Streza is a member of the firm Porter, Wright, Morris & Arthur, LLP in Cleveland. He has litigated product liability class actions, multi-district federal court product liability actions and complex individual product liability cases in state and federal courts. He received his law degree cum laude from the Cleveland-Marshall College of Law. He has taught trial and appellate advocacy as an adjunct professor at the Cleveland-Marshall College of Law.

L. Gino Marchetti, Jr. is a partner at Taylor, Pigue, Marchetti & McCaskill, PLLC in Nashville. His primary areas of practice include tax exempt entities, employment law, commercial and business litigation and corporate representation. He serves as a general counsel to various for-profit, as well as not-for-profit, entities, including the Roman Catholic Diocese of Nashville, Tennessee. He is a member of the IADC Executive Committee.

1. U.S. Const. Amend. I.
2. McClure II. 460 F.2d at 558
3. Watson v. Jones, 80 U.S. (13 Wall.) 679 (1872); Presbyterian Church v. Hull Church, 393 U.S. 440 (1969); Serbian Eastern Orthodox Diocese v. Milivojevich, 426 U.S. 696 (1976)

The "wall of separation" between Church and State underlying these important constitutional principles is particularly applicable to disputes such as those raised by the Plaintiffs in a case involving the relationship between a church and its ministers or priests:

> The relationship between an organized church and its ministers is its lifeblood. The minister is the chief instrument by which the church seeks to fulfill its purpose. Matters touching this relationship must necessarily by recognized as of prime ecclesiastical concern. Just as the initial function of selecting a minister is a matter of church administration and government, so are the functions which accompany such a selection. It is unavoidably true that these include the determination of a minister's salary, his place of assignment, and the duty he is to perform in the furtherance of the religious mission of the church.
>
> It has long been the practice of The Salvation Army, as with many other religious denominations, to determine these matters which deal with the very terms of a minister's calling. Such a practice must be classified as both basic and traditional.

McClure II[4] 460 F.2d at 558-559. Thus, in *McClure II* the Court upheld the dismissal of employment discrimination claims brought by Mrs. McClure, a former Salvation Army minister who was discharged by The Salvation Army. After reviewing the holdings in *Watson v. Jones*, as well as other subsequent precedents holding that matters of church government and administration are beyond the purview of civil authorities, the *McClure II* court found that application of the provisions of Title VII to the employment relationship between The Salvation Army and its former minister would result in an encroachment by the State into an area of religious freedom which is forbidden under the principles of the free exercise clause of the First Amendment:

> An application of the provisions of Title VII to the employment relationship which exists between The Salvation Army and Mrs. McClure, a church and its minister, would involve an investigation and review of these practices and decision and would, as a result, cause the State to intrude upon matters of church administration and government which have so many times before been pro claimed to be matters of the singular ecclesiastical concern. Control of strictly ecclesiastical matters could easily pass from the church to the State. The church would then be without the power to decide for itself, free from state interference, matters of church administration and government.[5] *McClure II*, 460 F.2d at 560.

The same reasoning was applied in the U.S. Supreme Court's decision in *Milivojevich*, rejecting the attempt by a defrocked bishop of the Serbian Eastern Orthodox Church to challenge his church's actions as being procedurally and substantively defective and in violation of the church's internal regulations. The Illinois Supreme Court held that the actions of the church were arbitrary and invalid. The U.S. Supreme Court reversed and found the action of the Illinois Court to be an impermissible interference by a civil court with the affairs of the church:

> The fallacy fatal to the judgment of the Illinois Supreme Court is that it rests upon an impermissible rejection of the decisions of the highest ecclesiastical tribunals of this hierarchical church upon the issues in dispute, and impermissibly substitutes its own inquiry into church polity and resolutions based thereon of those disputes.
>
> Consistently with the First and Fourteenth Amendments "civil courts do not inquire whether the relevant (hierarchical) church governing body has power under religious law (to decide such disputes) . . . . Such a

4. McClure II 460 F.2d at 558-559

5. McClure II, 460 F.2d at 560. The special protections attached to the religious freedom clauses of the First Amendment were recognized by Congress in 1993 by the passage of the Religious Freedom Restoration Act, 42 U.S.C. § 2000bb *et seq.* ("RFRA"). This Act codified the standard of review applied to adjudication of free exercise claims by requiring the government to demonstrate a compelling government interest applied in the least restrictive means in order to substantially burden a person's exercise of religion. *See* EEOC v. Catholic University of America, 83 F.3d455 (D.C. Cir. 1996) (holding inter alia that RFRA barred a Catholic nun's Title VII sex discrimination claim based on denial of tenure and that the application of secular standards to a church's employment of its ministers burdens the free exercise of religion.

> determination . . . frequently necessitates the interoperation of ambiguous religious law and usage. To permit civil courts to probe deeply enough into the allocation of power with a (hierarchical) church so as to decide . . . religious law (governing church polity) . . . would violate the First Amendment in much the same manner as civil determination of religious doctrine." *Milivojevich*, 426 U.S. at 708-709 (citation omitted).[6]

Many cases involving ministers accused of abuse directly invoke the doctrine, rules, regulations, administration and disciplinary process of the Catholic Church governing the relationship between the church and its bishops and its priests, all of which are clearly ecclesiastical matters.

The questions raised by the allegations in these cases as to what a Diocese did or did not do or should or should not have done, would require examination, interpretation and review of the doctrines, policies, rules and regulations of the Catholic Church. What are the Catholic Church's religious doctrines directly applicable to the conduct of its bishops in the appointment, disciplining, treatment and dismissal of a priest? How does the Catholic Church interpret its religious doctrines, policies, order and regulations enunciated in the Catholic Church's law and doctrine as it relates to the ordination, discipline, assignment and dismissal of its priests? How are the confidentiality provisions of these processes applied to its bishops and priests and were those applicable to the investigation and actions taken by the Diocese regarding a priest's conduct? Did the Diocese and its representatives follow the substantive and procedural policies and protocols of the Catholic Church for investigating and dealing with the allegations of misconduct in connection with their investigation of an accused priest? What were the bases for the decision of a Diocese to discipline, treat, assign and dismiss an accused priest? Resolution of these and other related questions underlying the Plaintiffs' allegations would thrust the Court into second-guessing the decisions of the Diocese to deal with and eventually dismiss a priest and examining the Diocese's interpretation of its own discipline, faith, and ecclesiastical rules as well as its internal organization and administration. This is the very type of inquiry and interference prohibited by *Milivojevich*, *McClure* and numerous other judicial precedents.

The fact that Plaintiffs may cast their claims in the form of common law torts for battery, outrageous conduct, negligence *per se* and negligent infliction of emotional distress does not remove these allegations from the principles of law prohibiting civil court interference with a church's ecclesiastical policies, rules, discipline and administration. The Supreme Court rejected the injunctive and declaratory claims brought by the defrocked Serbian Eastern Orthodox bishop in *Milivojevich*; the Fifth Circuit rejected the reinstatement and damage claims for employment discrimination asserted by a former minister of The Salvation Army in *McClure*; and other courts have adopted the same reasoning in rejecting common law tort claims brought by ministers against their churches.

In *Hutchison v. Thomas*,[7] 789 F.2d 392 (6th Cir. 1986), the Court refused to intervene in a dispute between a Methodist minister and his church involving Hutchison's claims that he was wrongfully expelled from his ministry by fraudulent, collusive or arbitrary application of the rules, laws and doctrinal provisions known in the Methodist religion as The Discipline. Hutchison claimed his church and several of its ministers and representatives acted improperly and misapplied Methodist rules and regulations governing the conduct of its ministers. Hutchison, like other Plaintiffs, framed his claims in the form of common

6. The Supreme Court has been particularly reluctant to interfere with a church's selection of its own ministers. *See, e.g.*, Gonzalez v. Roman Catholic Archbishop of Manila, 280 U.S. 1, 16 (1929) ("it is the function of the church authorities to determine what the essential qualifications of a chaplain are and whether the candidate possesses them"); Milivojevich, 426 U.S. at 717 ("questions of church discipline and the composition of the church hierarchy are at the core of ecclesiastical concern").

7. Hutchison v. Thomas, 789 F.2d 392 (6th Cir. 1986)

law torts (defamation, intentional infliction of emotional distress, and breach of contract). Relying on *Watson*, *Milivojevich* and related cases, the Court dismissed Hutchison's claims and refused to intervene in the relationship between Hutchison and the Methodist church:

> Appellant [Hutchison] is really seeking civil court review of subjective judgments made by religious officials and bodies that he had become "unappointable" due to recurring problems in his relationships with local congregations. This court cannot constitutionally intervene in such a dispute.[8]
> *Hutchison*, 789 F.2d at 393.

Similarly, in *Lewis v. Seventh Day Adventists Lake Region Conference*,[9] 978 F.2d 940 (6th Cir. 1992), the Court declined to exercise jurisdiction over common law tort claims for breach of contract, promissory estoppel, intentional infliction of emotional distress and loss of consortium brought by a former Seventh Day Adventist minister and his wife. The Court refused to intervene in the employment dispute between the Seventh Day Adventist Church and its minister:

> We conclude that the First Amendment bars civil courts from reviewing decisions of religious judicatory bodies relating to the employment of clergy. Even when, as here, the plaintiff alleges that the religious tribunal's decision was based on a misapplication of its own procedures and laws, the civil courts may not intervene.[10]

Id. at 942-943; see also *Natal v. Christian and Missionary Alliance*, 878 F.2d 1575 (1st Cir. 1989) (failure to state claim for losses of business and mental anguish by a clergyman); *Yaggie v. Indiana-Kentucky Synod Lutheran Church*, 860 F. Supp. 1194 (W.D. Ky. 1994), aff'd, 64 F.3d 664 (6th Cir. 1995) (no jurisdiction to hear claim of defamation brought by a Lutheran minister); cf. Paul v. Watchtower Bible & Tract Society of New York, Inc., 819 F.2d 875 (9th Cir.), cert. Denied, 484 U.S. 926 (1987) (summary judgment granted dismissing common law claims of defamation, invasion of privacy, fraud and outrageous conduct brought by disassociated member arising from church's requirement that members "shun" her).[11]

Even in the highly emotional cases involving clergy abuse, most courts have recognized this prohibition against state courts reviewing actions by a church regarding the assignment, treatment, discipline or dismissal of its clergy. The Tennessee Court of Appeals for the Middle Section in *Tidman v. Salvation Army*,[12] 1998 WL 391765 (Tenn.Ct.App.) dismissed the Plaintiffs' action on First Amendment grounds. The *Tidman* court cited with approval the doctrines espoused by *McClure*, *Milivojevich* and their progeny. The Court found particular substance in the case of *Higgins v. Maher*,[13] 210 Cal.App.3d, 1168, 258 Cal.Rptr. 757 (Cal.App. 1989). The Tennessee Court of Appeals cited with approval the basis for the dismissal of Plaintiff's claims in *Higgins*:

> Regardless of the church's motives or objectives, or the circumstances giving rise, we would probably agree that torts such as battery, false imprisonment or conversion cannot be perpetrated upon its members with civil impunity. We find, however, that at least in the context of Higgin's averments, the torts recited are simply too close to the peculiarly religious aspects of the transaction to be segregated and treated separately - as simple civil wrongs. The making of accusations of misconduct; the discussion of same within the order; the recommendation of psychological or medical treatment; the

8. *Id*. At 393

9. Lewis v. Seventh Day Adventists Lake Region Conference, 978 F.2d 940 (6th Cir. 1992)

10. *Id.* at 942-943

11. In Kreshik v. St. Nicholas Cathedral, 344 U.S. 94 (1952), legislation had been passed which transferred control of the Russian Orthodox churches in North American from the Patriarch of Moscow to officials selected by a convention of North American churches. The Supreme Court held the legislation to be an unconstitutional interference with the free exercise of religion. On remand, the New York Court of Appeals determined that the common law of New York prohibited the Patriarch's appointees from exercising the control granted to them by Canon Law. The Supreme Court again reversed, holding that the judiciary, as well as the legislature, was prevented by constitutional principles from interfering with the free exercise of religion. Kreshik v. St. Nicholas Cathedral, 363 U.S. 190 (1960).

12. Tidman v. Salvation Army, 1998 WL 391765 (Tenn.Ct.App.)

13. Higgins v. Maher, 210 Cal.App.3d, 1168, 258 Cal.Rptr. 757 (Cal.App. 1989).

> infliction, whether intentionally or negligently, of emotional distress - these are all activities and results which will often, if not usually, attend the difficult process by which priestly faculties are terminated. If our civil courts enter upon disputes between bishops and priests because of allegations of defamation, mental distress and invasion of privacy, it is difficult to conceive the termination case which could not result in a sustainable law suit.[14]

A plaintiffs' common law claims against a Diocese and its bishops fall squarely within the same category of claims brought by the Salvation Army minister in McClure, the Serbian Eastern Orthodox bishop in *Milivojevich*, the Methodist minister in Hutchison, the Seventh Day Adventist minister and his wife in *Lewis* and in numerous other actions brought by ministers against their churches and in litigation based upon a church's actions regarding a minister. Therefore Courts should decline jurisdiction over claims based on treatment by a Church of its ministers, for to do otherwise would be a constitutionally impermissible infringement of defendants' First Amendment religious freedom rights to deal with, assign and discipline it priests.

In his article in The Catholic Lawyer, Jeffrey Moon discusses the protection of documents and records of churches and other religious institutions.[15] Two cases involving the selection of ministers are instructive as to what limitations apply to civil courts in these types of disputes involving churches and religious organizations. The first ministerial non-selection case is *Minker v. Baltimore Annual Conference of United Methodist Church*,[16] where the court rejected the claims made by a Protestant minister that he had been refused a pastor's position because of his age and in breach of an implied contract.[17] The court stated that "any inquiry into the Church's reasons for asserting that Minker was not suited for a particular pastorship would constitute an excessive entanglement in its affairs." However, the Court went on to state that the plaintiff would be permitted to proceed with an *express* contract claim so long as he did not resort to "impermissible avenues of discovery," which were described as being those that would create an excessive entanglement.[18] The court was very explicit in this case: it limited the appropriate boundaries of litigation to only those areas legitimate for court inquiry and resolution, and then clearly limited permissible discovery to those areas.[19]

Similar reasoning was applied in *United Methodist Church v. White*.[20] In that case the court wrote: "The First Amendment's Establishment Clause and Free Exercise Clause grant churches immunity from civil discovery and trial under certain circumstances in order to avoid subjecting religious institutions to defending their religious beliefs and practices in a court of law."[21] Thus, when faced with these issues, the more easily one can fit a situation into the *Minker*/*White* mold, the more effectively one will be able to resist document or records discovery.

II. Keeping the Grand Jury Confessional Private: History Requires Secrecy

Consider the following scenarios:

I. After an extensive grand jury inquiry, a prosecutor of a major metropolitan area decides against seeking indictments of several clergymen because the indictments would be time barred by the applicable statute of limitations.

II. In preparation of an anticipated grand jury investigation, a prosecutor gathers an extensive file but decides to present only segments of the file to the grand jury. After some indictments are returned, the prosecutor sets aside that portion of his file not presented to the grand jury.

14. Tidman, citing Higgins at 1176
15. 39 Catholic Lawyer, No. 1, 27 (Winter 1999)
16. 894 F. 70 1354 (D.C. Cir. 1990)
17. *See id.* at 1358
18. *Id.*
19. *See id.* at 1358-60
20. 571 A. 70 790 (D.D.C. 1990)
21. *Id.* at 792

III. After an 18-month grand jury investigation, extended by the supervising court twice with six month terms, the grand jury does not believe any indictments of the clergy are appropriate based on the evidence presented to the grand jury.

IV. The criminal trials of several priests have ended in acquittals and the prosecutor does not seek an additional grand jury investigation into alleged sexual abuse of minors in his jurisdiction, despite public outcries of injustice.

Each of these situations involves factors that may cause an interested party to try to invade the grand jury proceedings, or obtain the prosecutor's file, both of which usually are not open to public review. In each instance, news media, indicted defendants, lay persons, putative plaintiffs, civil trial attorneys or others may have an interest in the information gathered for, or provided to, the grand jury. Through public records requests, discovery subpoenas or special proceedings, these individuals might attempt to gain access to the prosecutor's file to obtain either: the trial preparation files as they relate to evidence presented to the grand jury; evidence prepared for but not presented to the grand jury; or, evidence that was gathered for trial whether or not it was introduced at trial.

Legal objectives of promoting legitimate government investigation and protecting privacy of witnesses and of the unaccused have long justified maintaining secrecy of grand jury proceedings. These same goals have created exceptions to legal definitions of public records under open records laws. The shear anticipation of the results of a high profile grand jury investigation has caused anxiety and public ridicule of priests.[22] The media frenzy and the public spotlight shining on allegations of sexual abuse by Catholic clergy, has, in at least one instance, caused priests to be indicted for offenses that had nothing to do with an individual's function as a priest.[23]

The media attention and the corresponding public interest of the alleged abuse has fueled emotional arguments that this secrecy should be relaxed, especially when the grand jury efforts do not result in an indictment or where a prosecutor does not use its litigation file.[24] Despite the reality that only a small percentage of the clergy have been identified with this issue, a mindset has developed that as a class, priests are presumed to have been involved in abuse. This has caused serious erosion of the legal objective of preserving privacy of those investigated but not accused. Despite these circumstances, the media spotlight should not shine on what occurred before the grand jury or into the prosecutor's file.

Criminal Rule Six and its Exceptions

The vast majority of states have a criminal procedure rule or statute that prohibits grand jurors, government attorneys or their assistants from disclosing matters occurring before the grand jury, which is substantially similar to the provisions of Rule 6(e) of the Federal Rules of Criminal Procedure.[25] Matters occurring before the grand jury include identities of witnesses, jurors, or targets of the investigation, substance of testimony, actual transcripts, strategy, subpoenas issued, and direction or pattern of investigation and deliberations, and questions and concerns of jurors.[26]

22. Megan Garvey, Priest Accused of Abuse Dies in Apparent Suicide, Los Angeles Times, April 5, 2002.

23. Scott Hiaasen, *Priest Gets Probation For Paying Teen Boy For Sex*, The Plain Dealer, June 27, 2003.

24. *See e.g.*, *In re Investigation*, SD 03 075617, Cuyahoga County, Ohio Common Pleas.

25. In pertinent part, FED. R. CRIM. P. 6(e)(2) provides:
(2) **Secrecy**.
(A) No obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B).
(B) Unless these rules provide otherwise, the fol lowing persons must not disclose a matter occurring before the grand jury:
(i) a grand juror;
(ii) an interpreter;
(iii) a court reporter;
(iv) an operator of a recording device;
(v) a person who transcribes recorded testimony;
(vi) an attorney for the government; or
(vii) a person to whom disclosure is made under Rule 6(e)(3)(A)(ii) or (iii);

26. *In re Sealed Case* 98-3077, 151 F. 3d 1059, 1072 n. 12 (D.C. Cir. 1998); Samaritan Health Sys. v. Superior Court, 182 Ariz. 219, 895 P. 2d 131 (1994) (subpoenas issued by a grand jury and responsive documents not submitted to the grand jury protected from disclosure); but see, Phillips v. U. S., 843 F. 2d 438 (11th Cir. 1988) (documents obtained by a grand jury subpoena that were not submitted to the grand jury and which were determined not to indicate the pattern of the grand jury investigation was not a matter before the grand jury subject to secrecy requirements).

Secrecy of grand jury proceedings encourages witnesses to come forward and testify truthfully and freely, stops potential defendants from fleeing, promotes complete deliberation and protects targets from public knowledge that they were under investigation.[27] Where there has been a perception by a grand jury witness that the proceeding would not remain secret, i.e. where there is a threat of an actual impairment of grand jury secrecy, there may be "just cause" for refusing to testify before the grand jury.[28]

Despite the historical emphasis on secrecy, the obligation is not absolute and there are express statutory and judicially created exceptions to the prohibition against disclosure.[29] The court supervising the grand jury investigation may allow disclosure upon a showing of particular need but only after the court weighs the need for secrecy against the need for the information. The court decides whether justice can only be done by disclosure.[30] One of the express statutory exceptions is that matters before the grand jury may be disclosed when ordered by the court and preliminary to or in connection with a judicial proceeding.[31]

Disclosure Allowed by Express Exceptions

Many reported decisions relate to efforts by private parties to release grand jury materials preliminary to or in connection with a judicial proceeding. In *United States v. Procter & Gamble Co.*, the court balanced the competing needs for secrecy and disclosure by ruling that a private party must demonstrate need "with particularity," so that a court could "discretely and limitedly" lift the secrecy of the proceedings.[32] Need could be demonstrated if without the grand jury material "a defense would be greatly prejudiced or that without reference to it an injustice would be done."[33]

Subsequently, the Supreme Court refined the standard in *Dennis v. United States*.[34] The Dennis court held that the

27. United States v. Sells Eng'g, Inc., 463 U.S. 418, 424, 425 (1983); Douglas Oil Co. v. Petrol Stops Northwest, 441 U.S. 211, 219 (1979).

28. *See, In Re Grand Jury Proceedings*, 797 F.2d 906 (10th Cir. 1986) (upholding a witnesses refusal to testify where a new reporter stood at the door of the grand jury room). Witnesses who testify before the grand jury are free to waive their concerns about their participation in a grand jury investigation and they are not governed by the secrecy requirements and are allowed to freely discuss their testimony. *See*, Butterworth v. Smith, 494 U.S. 624, 634-636 (1990); United States v. Sells Eng'g, Inc., 463 U.S. 418, 424, 425 (1983).

29. *See*, FED. R. CRIM. P. 6(e)(3):

(3) **Exceptions.**

(A) Disclosure of a grand-jury matter--other than the grand jury's deliberations or any grand juror's vote--may be made to:

(i) an attorney for the government for use in performing that attorney's duty;

(ii) any government personnel--including those of a state or state subdivision or of an Indian tribe--that an attorney for the government considers necessary to assist in per forming that attorney's duty to enforce federal criminal law; or

(iii) a person authorized by 18 U.S.C. § 3322.

(B) A person to whom information is disclosed under Rule 6(e)(3)(A)(ii) may use that information only to assist an attorney for the government in performing that attorney's duty to enforce federal criminal law. An attorney for the government must promptly provide the court that impaneled the grand jury with the names of all persons to whom a disclosure has been made, and must certify that the attorney has advised those persons of their obligation of secrecy under this rule.

(C) An attorney for the government may disclose any grand-jury matter to another federal grand jury.

* * *

(E) The court may authorize disclosure--at a time, in a manner, and subject to any other conditions that it directs--of a grand-jury matter:

(i) preliminarily to or in connection with a judicial proceeding;

(ii) at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury;

(iii) at the request of the government if it shows that the matter may disclose a violation of state or Indian tribal criminal law, as long as the disclosure is to an appropriate state, state subdivision, or Indian tribal official for the purpose of enforcing that law; or

(iv) at the request of the government if it shows that the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, as long as the disclosure is to an appropriate military official for the purpose of enforcing that law.

See also, *In re Biaggi*, 478 F. 2d 489, 494 (2d Cir. 1973) (establishing that there are "special circumstances" in which release of grand jury materials is appropriate outside the boundaries of Rule 6(e)); *In re Hastings*, 735 F. 2d 1261 (11th Cir. 1984); *In re Grand Jury Proceedings, Miller Brewing Co.*, 687 F.2d 1079 (7th Cir. 1982) ("a court must balance the need of the party seeking disclosure against the effect such disclosure would have on the policies underlying grand jury secrecy.").

30. *See, e.g.* Petition for Disclosure of Evidence Presented to Franklin County Grand Juries in 1970, 63 Ohio St. 2d 212, 407 N.E. 2d 513 (holding that disclosure to a civil litigant could be made after a careful weighing of the need for secrecy and the needs of the civil litigant.)

31. *See, e.g.* Rule 6(e)(3)(E)(i).

32. United States v. Procter & Gamble Co., 356 U.S. 677 (1958).

33. *Id.* at 682, 683.

34. Dennis v. United States, 384 U.S. 855 (1966).

defendant in a criminal proceeding should have received the grand jury testimony of four witnesses who had appeared before the grand jury that investigated him several years earlier as the defendant demonstrated that it was likely the witnesses gave trial testimony that was inconsistent with their grand jury testimony. Because these four witnesses had testified in public concerning the same matters, and the grand jury had completed its investigation, "none of the reasons traditionally advanced to justify nondisclosure of grand jury minutes" applied to maintain the secrecy of the proceedings.[35]

The most often cited precedent of the Supreme Court is *Douglas Oil Co. v. Petrol Stops Northwest*, which concluded that the district court appropriately disclosed grand jury material requested by corporate defendants in a civil antitrust proceeding.[36] The Supreme Court recognized that the legal objective of secrecy was reduced, but not eliminated, after the grand jury investigation ends, finding:

> disclosure is appropriate only in those cases where the need for it outweighs the public interest in secrecy, and that the burden of demonstrating this balance rests upon the private party seeking disclosure. It is equally clear that as considerations justifying secrecy become less relevant, a party asserting a need for grand jury transcripts will have a lesser burden in showing justification.[37]

Does the Public Have a Right to Know?

In addition to the express exceptions found in Criminal Rule 6(e), the veil of secrecy has been lifted in isolated cases involving issues of great historical or public interest, but only after the petitioner for such release demonstrated exceptionally compelling reasons or "special circumstances."[38] An appellate court upheld the denial of disclosure based on allegedly important historical interests in *In re Craig*.[39] Craig involved a doctoral candidate writing a dissertation about a government official 48 years after he was accused of being a communist spy. The government official appeared before a grand jury to answer charges against him, but he was not indicted before he died. After his death, more evidence surfaced showing that information he had provided to the American Communist Party was funneled to foreign communist governments.

The federal appellate court described a court's role in deciding whether to make public the ordinarily secret proceedings of a grand jury investigation as "one of the broadest and most sensitive exercises of careful judgment a trial judge can make."[40] It did not establish a *per se* rule denying a "historical interest" exception to the secrecy presumption, but it articulated that such an interest carried an exceptional burden of persuasion:

> [T]he "special circumstances" test cannot be satisfied by a blanket assertion that the public has an interest in the information contained in the grand jury transcripts. Indeed, by concluding that "the 'public interest' exception urged by the Petitioner [that any garden-variety public interest compels disclosure if it outweighs the need for secrecy in the particular grand jury proceeding in question] would swallow the general rule of secrecy" the district court made clear it was not closing off all historical interest arguments...[41]

Recognizing that there was no "talismanic formula" to follow, the court identified many factors it deemed to be relevant whenever a court was "confronted with these highly discretionary and fact sensitive 'special circumstances'" requests:

> (i) the identity of the party seeking disclosure; (ii) whether the defendant to the grand jury proceeding or the government opposes the disclosure; (iii) why disclosure is being sought in the particular case; (iv) what

35. *Id*. at 872.

36. Douglas Oil Co. v. Petrol Stops Northwest, 441 U.S. 211, 219 (1979).

37. *Id.* at 223.

38. *See, e.g. In re American Historical Association*, 49 F. Supp 2d 274 (S.D.N.Y. 1999) (tailoring disclosure of several hundred pages of grand jury transcript testimony from two special grand juries convened in 1947 and 1950 relating to perjury indictments and ultimately convictions of Alger Hiss).

39. *In re Craig*, 131 F. 3d 99 (2nd Cir. 1997).

40. *Id.* at 104.

41. *Id.* at 105.

> specific information is being sought for dis closure; (v) how long ago the grand jury proceedings took place; (vi) the current status of the principals of the grand jury proceedings and that of their families; (vii) the extent to which the desired material - either permissibly or impermissibly - has been previously made public; (viii) whether witness to the grand jury proceedings who might be affected by disclosure are still alive; and (ix) the additional need for maintaining secrecy in the particular case in question.[42]

The court emphasized that the identity of the party seeking disclosure carries great weight: "if a third-party stranger wishes to obtain release of data about secret meetings over the objection of the defendant, who, perhaps, was never indicted by the grand jury, then the trial judge should be extremely hesitant to grant release of the grand jury material."[43]

Where the party seeking disclosure was the news media and the grand jury target objected to disclosure, and no indictment was returned, the California Supreme Court in *Daily Journal Corporation v. Superior Court*, reversed an order disclosing grand jury testimony.[44] The case arose out of the Orange County bankruptcy petition and a subsequent grand jury investigation of the underwriter of several debt offerings issued by the county. The underwriter provided testimony and documents over an eleven-month investigation, but no indictments followed because the underwriter entered into a civil settlement with the county on the eve of the grand jury deliberations.

The news media thereafter submitted a request for release of all grand jury material. Citing "the public's right to information under the First Amendment and the California Constitution" and the court's "inherent equity, supervisory and administrative powers," the court ordered disclosure due to "the magnitude of the public's loss of funds and loss of confidence in government and financial markets" and "each and every citizen's . . . inalienable right to the disclosure of this information."[45]

Unlike the majority of states, a California statute automatically provides for disclosure of grand jury proceedings to the public 10 days after an indicted defendant received a copy of the grand jury materials.[46] The automatic disclosure can be blocked but only if a defendant's right to a fair trial would be compromised by public disclosure.[47] The California Supreme Court held that the statute had no application where there was no indictment and the court applied the traditional reasons for secrecy surrounding grand jury proceedings.

> In the absence of an indictment, without the protections of the court process, the innocently accused and even witnesses are more vulnerable to a risk of adverse consequences ranging from reputational injury to retaliation. . . . we remain persuaded of the continuing importance of maintaining the heritage of grand jury secrecy when there has not been an indictment, in order to preserve the effectiveness of the grand jury process, as well as to protect witnesses against the adverse consequences, including damage to reputation, of disclosing their testimony.[48]

The California Supreme Court also held that absent statutory authorization, California courts have no "inherent" authority to disclose grand jury proceedings.[49] Furthermore, the court determined the public's "right to know" as a constitutional argument to be "unpersuasive."

The news media tackled head on the constitutionality of a Massachusetts statute that sealed all records of grand jury proceedings that resulted in a "no bill" - or a decision not to prosecute in *Globe Newspapers Company v. Pokaski*.[50] The press argued that it had a First Amendment

42. *Id.* at 106.
43. *Id.* at 106; the appellate court ultimately affirmed the trial court's sound exercise of discretion because there had not been an extensive exposure of grand jury proceedings by way of criminal trial testimony and because many of the grand jury witnesses would be identified. Id. at 107
44. Daily Journal Corp. v. Superior Court, 20 Cal. 4th 1117, 979 P. 2d 982 (1999).
45. *Id.* at 1121, 979 P. 2d at 984.
46. Cal. Penal Code §938.1
47. *Id.*
48. Daily Journal, 20 Cal. 4th at 1132, 979 P. 2d at 992.
49. *Id.* at 1128, 979 P. 2d at 989.
50. Globe Newspapers Co. v. Pokaski , 868 F. 2d 497 (1st Cir. 1989).

right to such records, especially where a press release or a publicly filed complaint preceded the grand jury proceeding. The press argued that an across the board sealing was impermissible and that the First Amendment required the court to conduct an analysis of each request for release of records in order to determine whether the release of such records would hinder the functioning of the grand jury process. The appellate court disagreed and held:

> The public has no right to attend grand jury proceedings, and therefore has no right to grand jury records. In contrast to criminal trials, grand jury proceedings have traditionally been closed to the public and the accused, and the Supreme Court has stated repeatedly that the proper functioning of our grand jury system depends on the secrecy of grand jury proceedings. . . . We conclude that, regardless of any prior publicity that may have occasioned a grand jury proceeding, the public has no constitutional right to the cases ending with a no bill, and therefore . . . the automatic sealing requirement is constitutional as applied to such records.[51]

Are Grand Jury Materials Available as Public Records?

As a general proposition, most records or documents in a prosecutor's file should be exempted from disclosure as confidential law enforcement investigation or as records gathered in reasonable anticipation of litigation - predominantly because these exemptions are intended to protect the personal privacy of citizens until their convictions become a matter of public record. A separate issue is whether a prosecutor can voluntarily disclose the contents of his file, regardless of the existence of a request.

In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court provided a detailed analysis of why records that filter through a prosecutor's file should not be disclosed to the public.[52] In this case, the Court unanimously reversed the federal appellate court for the District of Columbia. After the denial of its Freedom of Information Act ("FOIA") request, a national broadcasting news group and a public interest group filed suit in the district court seeking a private citizen's "rap sheet" compiled by the Federal Bureau of Investigation ("FBI"). The Pennsylvania Crime Commission had identified the citizen's family business as a legitimate business dominated by organized crime figures, and the business allegedly received numerous government contracts with a Congressman accused of corruption. The plaintiffs alleged that the public interest required disclosure of the rap sheet.

FBI rap sheet information is a compilation of publicly available data, but official distribution of the actual rap sheet is limited. The Supreme Court noted it was required to balance the Congressional intent of "full agency disclosure" against three "arguably relevant" exemptions found in the FOIA.[53]

The Supreme Court focused on the law enforcement compilation exemption and described it as a broader exemption than the other two arguably relevant exemptions. It then analyzed whether the citizen's interest in the nondisclosure of a rap sheet was the sort of "personal privacy" interest Congress intended to protect by the exemption. The Supreme Court rejected the plaintiff's claim that there was no privacy interest at stake because the information was a compilation of publicly available data as a "cramped notion of personal privacy."[54]

> Plainly, there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations through

51. *Id.* at 509, 511.

52. United States DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

53. "Exemption 3 applies to documents that are specifically exempted from disclosure by another statute. 5 U.S.C.S. § 552(b)(3). Exemption 6 protects personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C.S. § 552(b)(6). Exemption 7(C) excludes records or information compiled for law enforcement purposes, but only to the extent that the production of such materials could reasonably be expected to constitute an unwarranted invasion of personal privacy. 5 U.S.C.S. § 552(b)(7)(C)." *Id.* at 755-756.

54. *Id.* at 763.

> out the country and a computerized summary located in a single clearinghouse of information.
>
> * * *
>
> Both the common law and literal under standings of privacy encompass the individual's control of information concerning his or her person. . . . .the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. . . . According to Webster's [dictionary] initial definition, information may be classified as 'private' if it is 'intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public.'[55]

After defining the privacy interest at stake, the Supreme Court affirmatively recognized that the release of the rap sheet was an unwarranted invasion of personal privacy:

> Our previous decisions establish that whether an invasion of privacy is warranted cannot turn on the purposes for which the information is made. . . . the identity of the requesting party has no bearing on the merits of his or her FOIA request . . .. Thus whether disclosure of a private document . . . is warranted must turn on the nature of the requested document and its relationship to 'the basic purpose of the Freedom of Information Act to open agency action to the light of public scrutiny.'

The Supreme Court made clear that the "public interest" in law enforcement records about individuals was not the type of information afforded by the FOIA - and presumably by state public records laws. The purpose of open record laws, like FOIA, is to allow "public understanding of the operations and activities of the government" and not to allow a look into the lives of individuals investigated by the prosecutor.[56]

Several leading state court opinions follow this rationale. In *State, ex rel. Thompson Newspapers, Inc. v. Martin*, a newspaper sought to unseal a file related to a criminal investigation of a unidentified elected official.[57] The judge who sealed the file concluded that the file was exempted as a public record and as a confidential law enforcement investigatory record. The Ohio Supreme Court agreed: "[I]n order for law enforcement records to be subject to disclosure we have required some action beyond the investigatory stage where suspects have either been arrested, cited, or otherwise charged with an offense."[58] The decision not to file formal charges by the prosecutor against the suspect did not take the record outside the exception provided for confidential law enforcement investigatory records: "Just because formal charges were not filed in this instance does not change the status of the individual as a suspect . . .there is no reason why the suspect should be subjected to potential adverse publicity where he or she may otherwise have never been implicated in the investigation."[59]

Whether investigatory records or trial preparation materials are available after an acquittal or conviction has not been decided directly in any reported decision. From other fact patterns, such records should still remain confidential and exempt from public record disclosure. In *Daily Journal v. Police Department of Vineland*, the court refused to allow the newspaper to obtain police investigation reports that were presented to the grand jury.[60] The court held that the reports were lost their status as public records when the records were presented to the grand jury and aided the grand jury in returning indictments against the investigation targets. Thus, even though the identity of the targets of the investigation became public upon presentment of the indictments, the investigation files retained their non-public character.

In *Samaritan Health Systems v. Superior Court*, the Arizona Appellate Court ruled

55. *Id.* at 764.
56. *Id.* at 775.
57. State, ex rel. Thompson Newspapers, Inc. v. Martin, 47 Ohio St. 3d 28, 546 N.E. 2d 939 (1989).
58. *Id.* at 31, 546 N.E. 2d at 942.
59. *Id.*
60. Daily Journal v. Police Dept. of Vineland, 351 N. J. Super. 110, 797 A. 2d 186 (2002).

that the portion of the prosecutors' investigation file that was not presented to the grand jury remained secret, not as an exception to the public records law, but as a part of the grand jury proceeding. The Samaritan court reasoned: "The grand jury proceeding includes the preliminary review and investigation by the grand jury's agent, the prosecutor. . . . The public policy reasons for grand jury confidentiality apply to the case in which the grand jury does not review the material, as well as in those cases in which the grand jury reviews it and returns a no bill, or a true bill, i.e. an indictment."[61]

Conclusion

Despite the emotional nature of the allegations and the glaring publicity and international attention aimed at the clergy, public interest should not justify an invasion into the grand jury proceedings or the prosecutor's file. The time honored tradition in the United States, a tradition "older than our Nation itself,"[62] is that proceedings before the grand jury generally remain secret in order to continue the success and effectiveness of grand juries and the protection of witnesses who testify before them.

61. Samaritan Health Sys. v. Superior Court, 182 Ariz. 219; 895 P. 2d 131 (1994).

62. Pittsburgh Plate Glass Co. v. United States, 360 U.S. 395, 399 (1959).

The Privacy Project II

Personnel Records, Pedophiles and Priests: An Addendum to Discovery in Sexual Abuse Claims

By William G. Porter II and Michael C. Griffaton

Sunlight is said to be the best of disinfectants.[1]

For I must talk of murders, rapes, and massacres. Acts of black night, abominable deeds.[2]

To resist grand jury subpoenas, to suppress the names of offending clerics, to deny, to obfuscate, to explain away; that is the model of a criminal organization, not my church.[3]

Introduction

In the previous article, Ralph Streza and L. Gino Marchetti, Jr. discussed the constitutional issues that may limit (some would say, thwart) the discovery process in clergy molestation cases. Messrs. Streza and Marchetti specifically focused on the sanctity of grand jury proceedings and on restricting a plaintiff's access in a civil case from the information in those proceedings and in the prosecutor's file. As an addendum to Messrs. Streza and Marchetti's article, we discuss whether priests' personnel records are discoverable in civil molestation lawsuits.

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

Michael C. Griffaton is an associate in the same firm and concentrates in employment law. He is a graduate of Ohio Wesleyan University (1990) and Case Western Reserve University School of Law (1993). *The authors thank Ken Rubin, who clerked at Vorys during 2003, for his invaluable research on this topic.*

While there are reports of clergy of all faiths molesting children and adolescents, the Catholic Church institutionally has been involved in the most highly publicized cases and has borne the brunt of public indignation when such behavior comes to light.[4] This is not without cause as the scope of the priest sexual abuse scandal in the Boston Archdiocese makes pellucid.[5] Historically, the Catholic Church has dealt with accusations of priest pedophilia by counseling the accused priest, and then transferring him to another parish (often without informing that other parish of the

1. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY, AND HOW THE BANKERS USE IT 62 (Nat'l Home Libr. ed., 1933).

2. WILLIAM SHAKESPEARE, TITUS ANDRONICUS Act v, sc. 1, lines 63-64 (Gustav Cross ed., Penguin Books 1966) (1594).

3. Former Oklahoma Governor Keating made this statement when he resigned as chair from an independent board appointed by the U.S Catholic bishops that is charged with holding bishops publicly accountable for implementing policies to remove all abusive priests, protect children, support victims, and study the scope and causes of abuse. http://www.usatoday.com/news/nation/2003-06-16-keating_x.htm (last visited November 24, 2003).

4. *See* James T. O'Reilly and Joann M. Strasser, Clergy Sexual Misconduct: Confronting the Difficult Constitutional and Institutional Liability Issues, 7 ST. THOMAS L. REV. 31 (1994) (citing reports of clergy molestation by priests, rabbis, Presbyterian, evangelical, and Methodist ministers, and Buddhist teachers). While this article refers to the Catholic Church, the same issues apply to all clergy regardless of their religious affiliation.

5. "[I]t soon became clear that clergy abuse was, in fact, a systemic problem in the Boston Archdiocese, involving scores of priests and hundreds of victims across the metropolitan area." The Boston Globe website contains exhaustive documentation, including depositions and letters from priests' personnel files, pertaining to the priest sexual abuse scandal in the Boston Archdiocese. *See* http://www.boston.com/globe/spotlight/abuse/documents/ (last visited November 23, 2003).

priest's misdeeds), where frequently the priest molests again. This pattern has repeated itself again and again, in what has been called a Church cover-up. "Indeed, documents uncovered in lawsuits show bishops recommending the purging not of priests but of their personnel files, lest they become weapons in lawsuits."[6]

This is not surprising. When a priest is accused of molesting a child or adolescent, criminal prosecution and civil lawsuits soon follow. When these suits commence, plaintiffs and prosecutors are eager to see internal Church documents, especially personnel records of the accused priests and records of the Church's investigation and handling of the priest. In the many cases involving the Boston Archdiocese, for example, "thousands of pages of personnel documents detailed allegations of priests abusing women and girls and exchanging drugs for sex."[7] And in many cases, the Church has steadfastly resisted the disclosure of such documents.

The Church generally raises two defenses when faced with a motion to compel the production of personnel and related records. First, the Church argues that producing priests' personnel records violates the priest-penitent privilege. Failing that, the Church argues that the First Amendment to the United States Constitution and similar state constitutional provisions prohibit a court from interfering with the inner workings of the Church by compelling such production.

The Church has been consistently unsuccessful with both arguments. However, the courts recognize the Church's legitimate interests advanced in those positions. Consequently, courts balance those interests with plaintiffs' interests in full discovery by conducting *in camera* inspections of the requested documents to determine whether the documents are relevant and not otherwise privileged, and so discoverable, before disclosing them to plaintiffs.

I. The Purpose of Discovery

Parties may obtain discovery regarding any matter, not privilegedthat is relevant to the claim or defense of any party…[8]

One way in which the Catholic Church has attempted to resist discovery of relevant information in civil molestation actions is by placing personnel records and related information such as the Church's investigation and handling of prior complaints against the priest in a place that is designated by canon law as a "secret archive." According to the Code of Canon Law No. 489 of the Roman Catholic Church: "There is to be a secret archive ... or at least a safe or file in the ordinary archive, completely closed and locked and which cannot be removed from the place," for "documents to be kept [and] protected most securely." Canon 490 states further that "[o]nly the bishop" governing the diocese may possess the secret archive's key and that "documents are not to be removed from the secret archive or safe."[9]

It is axiomatic that the purpose of discovery is to bring out the facts prior to trial so the parties will be better equipped to decide what is actually at issue. The United States Supreme Court long ago noted that "[m]utual knowledge of all relevant facts gathered by both parties is essential to proper litigation."[10] Discovery is the logical method of preventing surprise and permitting both the court and counsel to have an intelligent grasp of the issues to be litigated and knowledge of the facts underlying them.

This is the prevailing view among the courts and the drafters of the state and fed-

6. Lisa M. Smith, *Lifting the Veil of Secrecy: Mandatory Child Abuse Reporting Statutes May Encourage the Catholic Church to Report Priests Who Molest Children*, 18 LAW & PSYCHOL. REV. 409, 412 (1994) (quoting Aric Press, et al., Priests and Abuse, NEWSWEEK, Aug. 16, 1993, at 42-43).

7. Kirk Enstrom, *Sex Abuse Scandal Rocks Catholic Church: Personnel Files Reveal Church Knowledge of Abusers*, (Dec. 24, 2002) http://www.thebostonchannel.com/news/1854448/detail.html (last visited November 24, 2003).

8. FED. R. CIV. P. 26.

9. *See* Hutchison v. Luddy, 414 Pa. Super. 138, 144-45 (1992).

10. Hickman v. Taylor, 329 U.S. 495, 507 (1947).

eral rules of civil procedure. As one court has noted, "[T]here has been a consistent trend since 1959 favoring broad pretrial discovery for the purpose of enabling litigants to prepare themselves fully for trial and to enhance their ability to present to the jury and the trial court all the pertinent facts and legal theories so that a just decision will be rendered."[11]

Likewise, Rule 26(A)(1) of the Ohio Rules of Civil Procedure provides that "[i]t is the policy of these rules to preserve the right of attorneys to prepare cases for trial with that degree of privacy necessary to encourage them to prepare their cases thoroughly and to investigate not only the favorable but the unfavorable aspects of such cases." In light of this, "[i]nsofar as the canons of the Church are in conflict with the law of the land, the canons must yield."[12] Simply placing information into a "secret archive," therefore, is not sufficient in itself to preclude discovery.

II. The Priest-Penitent Privilege

The mere fact that a communication was made to a clergyman or documentation was transmitted to a clergyman is insufficient in itself to invoke the privilege.[13]

In 1988, Samuel C. Hutchison commenced a civil action to recover damages against the Reverend Father Francis Luddy for alleged pedophilic sex acts performed while Father Luddy was serving as his priest. Hutchinson also alleged that the Bishop, several Monsignors, the local Diocese, and the Catholic Church had negligently hired or retained Father Luddy and had assigned him to a pastorate when they knew or should have known of his pedophilic tendencies. Hutchinson sought discovery of Luddy's personnel file as well as documents that pertained to actual reports of sexual involvement with minor male children by priests in the diocese. The Church resisted, claiming among other things, that the information was protected from disclosure under the priest-penitent privilege.[14]

As a doctrine of some faiths, including Roman Catholicism, clergy have an obligation to maintain the confidentiality of pastoral communications.[15] The clergy-penitent privilege is an evidentiary rule derived from the common law that protects a penitent's communications with his or her priest from revelation in court. The privilege is recognized in the United States by statute in every state and by the federal government.[16] As the United States Supreme Court explained, the privilege "recognizes the human need to disclose to a spiritual counselor, in…confidence, what are believed to be flawed acts or thoughts and to received priestly consolation and guidance in return."[17] Like all evidentiary privileges, the priest-penitent privilege is not absolute.[18]

Courts have limited the priest-penitent privilege in civil and criminal molestation cases. Pennsylvania courts, for example, "have interpreted [the] clergy-communicant privilege as applying only to confidential communications between a communicant and a member of the clergy in his or her roles as *confessor* and *spiritual counselor*."[19] The Pennsylvania Supreme Court, in determining the parameters of the privilege, found its "review of the relevant case law reveal[ed] no jurisdiction extending the privilege to communications that are not penitential or spiritual in nature."[20] Thus, in

11. Vythoulkas v. Vanderbilt University Hosp., 693 S.W.2d 350, 353 (Tenn. Ct. App. 1985).

12. Hutchinson, 414 Pa. Super. at 145.

13. *Id.* at 148.

14. *Id.* at 138.

15. Under the Code of Canon Law No. 1388, a priest who directly violates the seal of confession is automatically excommunicated and only the Holy See can lift the ban. *See* Fr. William P. Saunders, *Excommunication: A Call to Grace*, THE ARLINGTON CATHOLIC HERALD, (Feb. 20, 2003), available online at http://www.catholicherald.com/saunders/03ws/ws030220.htm (last visited November 25, 2003).

16. *See* Ronald J. Colombo, *Forgive Us Our Sins: The Inadequacies of the Clergy-Penitent Privilege*, 73 N.Y.U. L. REV. 225, 231 & n. 39 (1998) (collecting statutes); Cox v. Miller, 296 F.3d 89, 102 (2nd Cir. 2002).

17. Trammel v. U.S., 445 U.S. 40, 51 (1980).

18. "Evidentiary privileges are not favored; ... exceptions to the demand for every man's evidence are not lightly created nor expansively construed, for they are in derogation of the search for the truth." Herbert v. Lando, 441 U.S. 153, 175 (1979) (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974)).

19. Pennsylvania v. Stewart, 547 Pa. 277, 283 (Pa. 1997) (emphasis in original).

20. Stewart, 547 Pa. at 287.

many instances, the Church's knowledge of a priest's pedophilia would not be privileged because "Church leaders who receive information about sexual misconduct by clergy seldom learn of this information solely in a privileged setting, such as when the offending minister confesses or seeks spiritual counseling form his superior. Much more frequently, church leaders learn of the abuse from parents of the children affected, or other clergy members who are reporting misconduct by their peers."[21]

A notable exception to this involves the Catholic Church's Vicar of Priests, who serves as a confidant to priests in need of counsel and support regarding matters related to their position.[22] In *Corsie v. Campanalonga*, victims of alleged sexual molestation by a former priest sought production of documents contained in the priest's personnel files which were held by the Vicar. The court held that only statements made by the priest in confidence to the Vicar were protected by the priest-penitent privilege; other documents did not obtain a privileged or protected status simply because they were possessed by the Vicar.[23]

In *Hutchinson*, the court first determined that the information the plaintiff sought from the Church pertaining to Father Luddy's alleged sexual molestation was relevant to his claims. Similarly, the circumstances involved in the Church's handling of Father Luddy and other named priests who were known to be pedophilic would be relevant to plaintiff's claim that the Church was negligent in concealing such tendencies and that this contributed causally to his own molestation.[24] The court then found that the information sought was not privileged because there was no evidence that the information was privileged within the meaning of Pennsylvania's statutory clergy-penitent privilege. "This privilege protects 'priest-penitent' communications; it does not protect information regarding the manner in which a religious institution conducts its affairs or information acquired by a church as a result of independent investigations not involving confidential communications between priest and penitent."[25] The court next addressed the Church's contention that the documents sought were protected from disclosure by the First Amendment.

III. The First Amendment

Although the freedom to believe is absolute, the freedom to act cannot be.[26]

The Establishment and Free Exercise Clauses of the First Amendment prohibit excessive government entanglement with religious organizations. The First Amendment "forbids civil courts from deciding issues of religious doctrine or ecclesiastical polity."[27] Courts have long held that civil courts lack jurisdiction over purely spiritual matters, the administration of church affairs that do not affect the civil or property rights of individuals, internal church conflicts, and the imposition of church-related discipline on its members.[28] This is because there is a perceived danger that in resolving intrachurch disputes the state will become entangled in essentially religious controversies or intervene on behalf of groups espousing particular doctrinal beliefs.[29]

At the same time, the courts have consistently held that the First Amendment is not a defense to disclosure of personnel records. Unlike reviewing a Church's decision whether and how severely to discipline a member, for example, priest sexual abuses cases do not require interpreting or weighing Church doctrine and neutral prin-

21. R. Michael Cassidy, *Sharing Sacred Secrets: Is It (Past) Time for a Dangerous Person Exception to the Clergy-Penitent Privilege?*, 44 WM. & MARY L. REV. 1627, 1699 (2003).

22. Corsie v. Campanalonga, 317 N.J. Super. 177, 182 (N.J. Super. A.D. 1998).

23. *Id.*

24. Hutchinson, 414 Pa. Super. at 146.

25. *Id.* at 147.

26. Alberts v. Devine, 395 Mass. 59, 73 (1985) (quoting Attorney General v. Bailey, 386 Mass. 367, 375 (1982)) (internal quotation marks omitted).

27. Elmora Hebrew Ctr., Inc. v. Fishman, 125 N.J. 404, 413 (N.J. 1991).

28. *See, e.g.*, Chavis v. Rowe, 93 N.J. 103, 109 (N.J. 1983); Hutchison v. Luddy, 414 Pa. Super. 138 (Pa. Super. Ct. 1992);.

29. *See* The Serbian Eastern Orthodox Diocese for the United States of America and Canada v. Milivojevich, 426 U.S. 696, 709-10 (1976).

ciples of law (i.e., the rules of discovery) can be applied. In *Corsie v. Campanalonga*, the New Jersey Court of Appeals aptly summarized this view:

> [T]he maintenance of personnel files, generally speaking, is nothing more than a normal administrative procedure of any organization, whether it be religious or secular. It can hardly be argued that the ordinary maintenance of such files is a practice which is rooted in religious belief. Maintenance of the files does not involve religious doctrine. Discovery would not impinge upon the administration of the church or its customs or its practices. There is no usurpation of the decision-making function of a religious organization. Simply put, there is no religious dispute involved in the production of personnel files in the discovery phase of trial. Thus, there is no occasion for the church defendants to claim a privilege of nondisclosure under the First Amendment.[30]

Similarly, courts have rejected the Church's attempt to use the First Amendment to cloak any and all documents contained in the Church's "secret archive" with inviolate protection from disclosure. In *Hutchinson*, the Church argued that the First Amendment precluded the disclosure of such documents. The trial court noted that "[t]he relevant inquiry is not whether the Church gives a file a particular name, but whether disclosure of the information requested from that file interferes with the exercise of religious freedom."[31] The appellate court agreed-finding that there "is not one iota of evidence" that the court-ordered discovery of documents in the secret archive will impermissibly intrude upon either theological doctrine or the practice of religion.[32]

Conclusion

The discovery of documents deemed relevant and non-privileged does not impermissibly intrude upon the Church's exercise of its religious beliefs and practices.[33] Courts have rejected the Catholic Church's claim that personnel records of pedophiliac priests are protected from disclosure by the First Amendment. At the same time, the courts have also narrowly construed the priest-penitent privilege to permit the disclosure of priests' personnel files in civil litigation. To balance the competing interests against excessive entanglement in Church affairs with a plaintiff's need for full discovery, courts often conduct *in camera* review of the requested Church documents, whether they are personnel records or other records from the Church's "secret archive." In *Corsie*, for example, the appellate court directed the trial judge to conduct an *in camera* review of documents to determine if the requested documents were privileged, were relevant to plaintiffs' claims, or involved the privacy interests of unrelated third parties.[34]

30. *Id.* at 185-86 (internal citations omitted).
31. Hutchinson, 414 Pa. Super. at 152.
32. *Id.*
33. Pennsylvania v. Stewart, 547 Pa. 277, 291 (Pa. 1997); Niemann v. Cooley, 93 Ohio App.3d 81, 89-92 (Ohio App. 1 Dist. 1994).
34. Corsie v. Campanalonga, 317 N.J. Super. 177, 182 (N.J. Super. A.D. 1998).

The Privacy Project II

Family Unity or Family Crisis: Revisiting the Need for a Parent-Child Communication Privilege

By Mark D. Fox and Michael L. Fox

"Privilege" is derived from the Latin phrase, "privata lex."...Although privata lex was a term developed in the days of ancient Rome, privileges protecting special relationships existed centuries before Rome coined a term for them. [1]

I. Introduction: The Privilege Rules in Evidence

Americans take pride in having a justice system that has as one of its foremost and most professed goals the protection of individual rights. We also profess a true concern for the maintenance of family solidarity and values, and the protection and preservation of those values from intrusion. While few would argue our commitments to these goals, that commitment becomes less credible when re-examined in the context of the state of our law regarding the protection of confidences and communications exchanged between children and their parents.

In the United States, and the several States, there exist a number of both settled and unsettled evidentiary privileges. Among them are the Attorney-Client Privilege, the Physician-Patient Privilege, the Psychotherapist/Psychologist-Patient Privilege, the Clergy-Penitent Privilege, and the dual Spousal Immunity and Confidential Marital Communication Privileges. In the Federal Courts of the United States, either State or Federal Rules may govern evidentiary matters of privilege, depending upon the application of choice of law provisions - whether or not, in a civil matter, "State law supplies the rule of decision" - and the application of the *Erie* doctrine and the line of cases stemming from it.[2] However, at least one United States Court of Appeals has ruled that the *Federal Rules* will apply if a federal court case presents both state law and federal law claims - any other result would be "unworkable."[3] If the Federal Rules govern in a particular case, *Federal Rule of Evidence* 501 applies to all issues concerning testimonial privileges. However, the rules are often non-specific when it comes to establishing such privileges. For example, in relevant part, Rule 501 states:

Mark D. Fox: United States Magistrate Judge, United States District Court for the Southern District of New York. Former member of the Committee on Security and Facilities, Judicial Conference of the United States (1996-2002). JD, 1967, Brooklyn Law School; BA, 1964, State University of New York at Buffalo.

Michael L. Fox: JD, 2003, Harlan Fiske Stone Scholar, Columbia University School of Law; BA, 2000, summa cum laude and Phi Beta Kappa, Bucknell University. Litigation Associate with the law firm of Stroock & Stroock & Lavan LLP, in Manhattan (awaiting admission to the New York State Bar as of the date of publication). (This article reflects the thinking and opinions of the author alone, and does not reflect the positions or opinions of Stroock & Stroock & Lavan LLP, or any of its attorneys.)

1. Wendy Meredith Watts, *The Parent-Child Privileges: Hardly a New or Revolutionary Concept*, 28 WM. & MARY L. REV. 583, 590 (1987).

2. FED. R. EVID. 501 (2002); and *see* Erie v. Tompkins, 304 U.S. 64 (1938). Among those cases stemming from the Court's Erie decision include the seminal choice of law and procedure case Hanna v. Plumer, 380 U.S. 460 (1965).

3. Pearson v. Miller, 211 F.3d 57, 66 (3d Cir. 2000) (citing Wm. T. Thompson Co. v. General Nutrition Corp., 671 F.2d 100, 104 (3d Cir. 1982)).

> Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness [or] person…shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness [or] person…shall be determined in accordance with State law.[4]

In other words, the *Federal Rules* contain no particular or specified privileges. At one time, during the 1970's, Congress set out to codify certain privileges in the *Federal Rules*, among them the Attorney-Client Privilege (later proposed Rule 503), the Spousal Privilege (later proposed Rule 505), and the Clergy-Penitent Privilege (later proposed Rule 506). This attempt at codification failed, however, and left us only with the generality of Rule 501, *supra*.[5] To identify privileges under the *Federal Rules*, therefore, one must look either to case law or to federal statutes. Similarly, in New York, *Civil Practice Law and Rules ("CPLR")* section 3101 states, in relevant part: "Privileged matter. Upon objection by a party privileged matter shall not be obtainable."[6] Nothing more is stated on the issue in this section of the *CPLR*. The commentary to § 3101(b) acknowledges that this section simply invokes the rules of evidence normally applied in court, and then refers the reader to the law of evidence on privileges, specifically Article 45 of the *CPLR*.[7] But, neither Article 45 nor the *Federal Rules* contain a statutory Parent-Child Privilege - a protective device that could be applied to shield parents and children from being forced to testify against each other. The comment to section 3101(b) does state, however, that "any evidentiary exemption that fits broadly under the 'privileged' category, whether it emanates from CPLR Article 45 or any other law (or the constitution itself), is within CPLR 3101(b)."[8] This broadening language has cleared the way for a few lower court cases in New York that have expanded on a familial or parent-child evidentiary privilege - as we will see below. Furthermore, there is a guiding principle concerning the creation and existence of the evidentiary privileges, recently reaffirmed by the United States Court of Appeals for the Second Circuit, that should be kept in mind throughout this article:

> Because claims of privilege derogate from the public's "'right to every [person's] evidence,'"[sic]… "they must be strictly construed and accepted 'only to the very limited extent that permitting a refusal to testify or excluding relevant evidence has a public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth,'"[sic].[9]

Many cases and law review and journal articles have discussed, proposed, defended or refuted the need for or existence of testimonial privileges, including a parent-child privilege.[10] The law of privacy and of priv-

4. FED. R. EVID. 501 (2002).

5. Yolanda L. Ayala & Thomas C. Martyn, *To Tell or Not to Tell? An Analysis of Testimonial Privileges: The Parent-Child and Reporter's Privileges*, 9 ST. JOHN'S J. LEGAL COMMENT. 163, 166 & n. 9 (1993).

6. N.Y. C.P.L.R. 3101(b) (McKinney 2002).

7. N.Y. C.P.L.R. 3101(b), cmt. C3101:25 (McKinney 2002).

8. *Id.*

9. Cox v. Miller, 296 F.3d 89, 107 (2d Cir. 2002).

10. Among the many cases and articles are: Jaffee v. Redmond, 518 U.S. 1 (1996); Trammel v. United States, 445 U.S. 40 (1980); *In re Grand Jury*, 103 F.3d 1140 (3d Cir. 1997); *In re Erato*, 2 F.3d 11 (2d Cir. 1993); Port v. Heard, 764 F.2d 423 (5th Cir. 1985); United States v. Ismail, 756 F.2d 1253 (6th Cir. 1985); *In re Matthews*, 714 F.2d 223 (2d Cir. 1983); United States v. Jones, 683 F.2d 817 (4th Cir. 1982); Clark v. Greiner, No. 97-CV-2483(JG), 2001 WL 135732 (E.D.N.Y. Feb. 2, 2001); *In re Agosto*, 553 F.Supp. 1298 (D. Nev. 1983); *In re Greenberg*, 11 Fed. R. Evid. Serv. (Callaghan) 579 (D. Conn. 1982); State v. Anderson, 28 P.3d 662 (Or. Ct. App. 2001); Bond v. Albin, 28 P.3d 394 (Kan. Ct. App. 2000); *In re E.F.*, 740 A.2d 547 (D.C. 1999); *In re Ryan*, 474 N.Y.S.2d 931 (N.Y. Fam. Ct. 1984); Three Juveniles v. Commonwealth, 455 N.E.2d 1203 (Mass. 1983); People v. Harrell, 450 N.Y.S.2d 501 (2d Dept. 1982), aff'd, 449 N.E.2d 1263 (N.Y. 1983) (declining to rule on the privilege issue); People v. Fitgerald, 422 N.Y.S.2d 309 (Cty. Ct., Westchester Cty., 1979); *In re Application of A. & M.*, 403 N.Y.S.2d 375 (4th Dept. 1978); Susan Levine, Comments, *The Child-Parent Privilege: A Proposal*, 47 FORD. L. REV. 771 (1978-79); Ann M. Stanton, *Child-Parent Privilege for Confidential Communications: An Examination and Proposal*, 16 FAM. L.Q. 1 (1982); Ellen Kandoian, *The Parent-Child Privilege and Parent-Child Crime: Observations on* State v. DeLong *and* In re *Agosto*, 36 ME. L. REV. 59 (1984); Philip Kraft, *The Parent-Child Testimonial Privilege: Who's Minding the Kids?*, 18 FAM. L.Q. 505 (1985); Watts, *supra* note 1; and Ayala & Martyn, *supra* note 5. Mueller & Kirkpatrick also provide an informative and in-depth discussion of the status of familial privilege in their treatise on federal evidence. CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, 2 FEDERAL EVIDENCE § 208 (2d ed. 1994).

ileges ("privata lex") has existed for several millennia, and none of the issues addressed herein are novel ideas. Professors Watts, Stanton and Kraft, and Ms. Levine, have presented their own proposals for a Parent-Child Privilege statute, with defenses and justifications, in their respective articles. However, because little has been accomplished in the past several decades since their articles were written, we felt that it was time to re-ignite the debate. In doing so, we have re-thought the privilege, and set forth in Section III, *infra*, a set of proposed guidelines that we feel should be incorporated into an appropriate and necessary Parent-Child Privilege Statute. While reference is made to the works of Watts, Stanton, Levine and others, in attempting to outline and create a workable, recognized and protective privilege for families (other than spouses), this article proposes a privilege narrowed in some respects and broadened in others, and constructed with the express purpose of uniting the two sides of the road on a median of both public justice and privacy. For purposes of this discussion, a brief overview of the state of the law on the issue of familial evidentiary privilege will be helpful. Then, after consideration of the law at both the state and federal levels, we propose the establishment of a Parent-Child Confidential Communication Privilege for the readers' consideration. The proposed privilege will be strong, shielding, and more reasonable than some of the all-or-nothing privileges sought by litigants in the cases, or discussed by authors in the reviews and journals.

II. The Current Status of the Parent-Child Privilege

The legal history of a Parent-Child Privilege[11] is, apparently, a contentious one. However, in the Federal courts alone there is but one well-worn path, and that path leads away from any full-fledged recognition of a parent-child privilege in the law of evidence.[12] The Supreme Court of the United States has never squarely ruled on the existence of such a privilege, and the United States Congress has passed no legislation on the issue in conjunction with the provisions of Federal Rule 501. In fact, no federal appeals court has expressly acknowledged the existence of any sort of parent-child privilege in the law of evidence. Only certain select rulings from two United States district courts have attempted to expand the field, and shield parents and children from compelled testimony by or against family members.[13] But, unfortunately the Courts of Appeals have subsequently disapproved of these lower court rulings.[14]

Among the States, only four have recognized some form of a parent-child privilege, either through common law decisions or legislative action. No High Court of any state has recognized the existence of, or has offered to create, a parent-child privilege. [15] And, do not think that the decisional importance of this lack of positive federal and state case law has been lost on other courts.[16] In actuality, only New York State, by way of the rulings of several of its lower courts, recognizes the existence of a judicially-created parent-child privilege to some extent. At the same time, Idaho and

11. While we use "Parent-Child Privilege" as a shorthand label, this Privilege should be made to apply to parents or to legal guardians - whomever is legally responsible for the welfare and upbringing of the child.

12. *In re Grand Jury*, 103 F.3d 1140, 1146 (3d Cir. 1997).

13. *In re Agosto*, 553 F.Supp. 1298 (D. Nev. 1983); and *In re Greenberg*, 11 Fed. R. Evid. Serv. (Callaghan) 579 (D. Conn. 1982).

14. MUELLER & KIRKPATRICK, *supra* note 10, at § 208 & n.9.

15. The New York State Court of Appeals has heard two appeals in cases that included a claim of parent-child privilege. However, in the first case the Court determined that because no objection, as to the confidential communication between defendant and his mother, was raised at either the suppression hearing or at trial, the claim for the privilege had not been properly preserved for appeal. Thus, despite a ruling by the Second Department below, the Court of Appeals declined to rule on the existence or non-existence of the parent-child privilege in the common law of the State of New York. People v. Harrell, 449 N.E.2d 1263 (N.Y. 1983). In the second case the Court, while not expressly stating that a privilege either does or does not exist for parent-child communication, held that the privilege would likely not apply to a defendant who is not a minor, whose communications were made in the presence of other family members, whose mother freely testified before the Grand Jury, and whose crime was against another member of the household. People v. Johnson, 644 N.E.2d 1378 (N.Y. 1994). But, to this day we lack any definitive and affirmative ruling by the High Court on the matter of a parent-child privilege.

16. *In re Grand Jury*, 103 F.3d 1140, 1146 (3d Cir. 1997); In re E.F., 740 A.2d 547, 549 (D.C. 1999).

Minnesota are the only two states out of the fifty in the Union that have acted through their legislatures to create a limited Parent-Child Privilege.[17] Massachusetts has a statute that prevents a minor child from forced testimony against a parent in a *criminal* case, but the statute does *not* recognize an actual parent-child privilege. Rather, the statute has been characterized as a witness-disqualification rule, and it is said that the statute only applies to minors, and only under certain conditions.[18] Still other state courts and legislatures refuse to recognize a parent-child privilege at all.

Even in the states where the privilege has been acknowledged, it is at best barely viable. One can look to the case law of New York as a standard by which to measure the success of those who advocate the creation of the privilege. Though the New York Court of Appeals has not yet ruled on the issue, a few trial courts in New York have created or acknowledged the privilege, along with one or two of the Appellate Divisions. In March 1978, the Appellate Division, Fourth Department, a panel comprised of then-Presiding Justice Cardamone and Justices Simons, Dillon, Denman and Witmer, handed down a decision that was the first to recognize something resembling a parent-child privilege.[19] *A.&M.* concerned an important issue - whether parents could be required to testify before a Grand Jury as to communications made to them in confidence by their minor son. At the time, the Court admitted the issue was one of first impression in New York.[20] The son was accused of arson at a local college, and it was suspected by prosecutors that the son, seeking guidance, went to his parents - a "first stop" that many in such a situation are likely to make. His parents were not at the scene of the fire, and therefore were not being sought by the State to testify as to overt acts witnessed, but only to testify as to communications made between the parents and the child. The Erie County Court both expanded the marital privilege to encompass communications from children made in the privacy of the home, and found a basis for constitutionally protected privacy, thereby quashing the subpoenas that had been served on the parents.[21] The Fourth Department reversed the lower court on the expansion of the marital privilege, and also reversed the lower court on the law, remitting the matter for further proceedings. But, the Court did not completely denounce a protectable interest in private communications between parents and children. Instead, the Court ruled,

> Although the communication is not protected by a statutory privilege, we do not conclude that it may not be shielded from disclosure. It would be difficult to think of a situation which more strikingly embodies the intimate and confidential relationship which exists among family members than that in which a troubled young person, perhaps beset with remorse and guilt, turns for counsel and guidance to his mother and father. There is nothing more natural, more consistent with our concept of the parental role, than that a child may rely on his parents for help and advice. Shall it be said to those parents, "Listen to your son at the risk of being compelled to testify about his confidences?"[22]

The Court acknowledged that there is a certain "realm of family life which the state cannot enter," and cited United States Supreme Court precedent concerning parental responsibilities for the education, care, nurturing, and custody of children that fall within the ambit of constitutional privacy, and emanate from the "penumbra" of specifically enumerated constitutional

17.103 F.3d at 1146 & nn.13, 15 (citing, among others, *In re Ryan*, 474 N.Y.S.2d 931 (N.Y. Fam. Ct. 1984); People v. Harrell, 450 N.Y.S.2d 501 (2d Dept. 1982); and People v. Fitgerald, 422 N.Y.S.2d 309 (Cty. Ct., Westchester Cty., 1979); Idaho Code § 9-203(7) (1990 & Supp. 1995) (2003); and Minn. Stat. § 595.02(1)(j) (1988 & Supp. 1996) (2003)).

18.103 F.3d at 1146, n.13 (citing Mass. Gen. L. ch. 233, § 20 (1986 & Supp. 1996) (2003)). This Massachusetts statute was passed in response to the case *Three Juveniles*, 455 N.E.2d 1203 (Mass. 1983), in which the Court ruled that children would have to testify against their father in his trial for murder. The Court granted no privilege or disqualification to the children, so the Legislature chose to act and pass this somewhat weak and narrow statute. *See* Ayala & Martyn, *supra* note 5, at 170.

19. *In re Application of A. & M.*, 403 N.Y.S.2d 375 (4th Dept. 1978).

20. 403 N.Y.S.2d at 377.

21. *Id.* at 377.

22. *Id.* at 378 (emphasis added).

rights, thereby creating autonomy for the family unit.[23] The realm of family unity and the issue of privacy can be employed to protect communications between child and parent from being used as ammunition by opposing counsel. In order to invade the family unit, "the governmental needs asserted must be carefully examined in order to insure that there exists a legitimate purpose in abridging [the] familial interest."[24] The Court held that the integrity of the family is entitled to constitutional protection, and cites several authorities that emphatically state the importance of parents and children being able to "talk out" problems and concerns in a confidential and trusting environment, enabling the children to properly develop emotionally and mentally in relation to the world around them.[25]

Indeed, as Justice Denman wrote for the Court,

> If we accept the proposition that the fostering of a confidential parent-child relationship is necessary to the child's development of a positive system of values…there can be no doubt what the effect on that relationship would be if the State could compel parents to disclose information given to them in the context of that confidential setting. Surely the thought of the State forcing a mother and father to reveal their child's alleged mis deeds, as *confessed to them in private*, to provide the basis for criminal charges [or civil damages] is *shocking to our sense of decency, fairness and propriety*.[26]

While the *A.&M.* Court did not expressly create a privilege for parent-child communications, in closing its decision the Court illuminated the path to be taken in order for constitutional protection to be extended to parent-child communications:

> …we believe that the creation of a privilege devolves exclusively on the Legislature. We conclude, however, that communications made by a minor child to his parents within the context of the family relationship may, under some circumstances, lie within the "private realm of family life which the state cannot enter." That is not to say, however, that parents in this setting are immune from Grand Jury process. When a witness is sum moned to the Grand Jury by subpoena ad testificandum, he…may assert a privilege at the time of questioning, CPL 190.30(1),(5) ….There is no invasion of privacy in requiring the respondents to appear before the Grand Jury….there may be questions… which would not invade the area of family confidentiality….When respondents appear before the Grand Jury, they will be entitled to the advice of counsel…and may then assert their constitutional rights…when and if they are asked questions concerning communications made to them by their son in confidence. If the court is then asked to rule on such claim, it may find it necessary to hold an evidentiary hearing to determine whether the factual context in which the statements were made mandates that the information sought be given constitutional protection….[27]

However, just eight months later, in November of 1978, another panel of the Fourth Department, including Justices Cardamone, Simons and Witmer (who also presided over the *A.&M.* case), rejected the application of a parent-child privilege to a communication made from a son to his father concerning the son's guilt for the crime of criminal mischief.[28] The trial court had overruled defendant's objection of privilege to the questioning of his father concerning son's admissions, and following the father's testimony enough corroborating evidence existed to secure a conviction. The Fourth Department, citing to *A.&M.*, reaffirmed that no statutory parent-child privilege exists in New York, and that constitutional protection may only be extended to communications in limited circumstances. The Court concluded, though, that such circumstances did not exist in the case at Bar, finding that "[i]t does not appear that respondent made the statement to his father

23. *Id.* at 378-379 (citing, among others, Pierce v. Society of Sisters, 268 U.S. 510; Roe v. Wade, 410 U.S. 113; Wisconsin v. Yoder, 406 U.S. 205; and Griswold v. Connecticut, 381 U.S. 479).

24. 403 N.Y.S.2d at 378.

25. *Id.* at 380.

26. *Id.* at 380 (emphasis added).

27. *Id.* at 381-382 (internal citations omitted).

28. In the Matter of Mark G., 410 N.Y.S.2d 464 (4th Dept. 1978).

in confidence and for the purpose of obtaining support, advice or guidance…"; and the Court also found that the father's willingness to testify to the son's admissions at trial illustrated that he did not otherwise wish to remain silent or keep his son's confidences private.[29]

One year after *Mark G.*, another New York Court advanced the parent-child privilege with a firm step forward. In November 1979, County Court Judge Gerard Delaney, of Westchester County, decided the seminal case of *People v. Fitzgerald*.[30] Following remand from an earlier appeal, a second trial was had on the charges of criminally negligent homicide and third degree assault. Testimony was sought from the father of the 23-year-old defendant, after it was discovered that the two had had a private Christmas Eve conversation about the accident from which the charges stemmed. The Court faced a question of "whether there exists a 'parent-child' privilege which would prevent forced disclosure by the State of confidential communications between a parent and a child of any age when the parties to such communication *mutually assert such a privilege*."[31] Judge Delaney ruled that "such a privilege *can and does exist*, grounded in *law, logic, morality and ethics*," and found protection stemming directly from both the Federal and State Constitutions and the "right to privacy" - a protection the judge found to be so compelling that the privilege was broadened by the Court to include children of any age still engaged in familial relationships with parents, since the State may not erect "artificial barriers" to facilitate the overturning of constitutional protections.[32] In support of its ruling, the Court cited authorities from across the board, including those stating that privileges are designed to "protect relationships deemed socially desirable," that it has been established that the Constitution "protects the sanctity of the family," and that the courts cannot hide behind the "tendency" not to expand the categories of privileges while disregarding "situations where the foundations of certain Basic relationships, such as those between family members may be threatened."[33] And, in citing *A.&M.*, the Court reiterated that,

> if it is determined that the information sought…was divulged by the (child) in the context of the familial setting for the purpose of obtaining support, advice or guidance …(then) the interest of society in protecting and nurturing the parent-child relationship is of such overwhelming significance that the State interest in fact-finding must give way.[34]

Judge Delaney also ruled that since the protections flow directly from both Constitutions, and federally protected rights, the issue of a parent-child privilege is a *matter of law*, fit for a *court* to decide regardless of whether or not the Legislature chooses to act.[35] This opinion can be cited in opposition to the many other court decisions from across the nation that leave the creation of new privileges, especially the contested Parent-Child Privilege, exclusively in the hands of legislatures.

The final two New York cases, which fill in the field, serve to both expand and solidify the common law privilege established by those few progressive judges. First, in *People v. Harrell*,[36] the Appellate Division, Second Department, dealt with a claim of parent-child privilege arising from a conversation between an arrested youth and his mother, in a police station, that was overheard by an officer. The Court determined that the law prevents the police from isolating a minor from contact with his or her parents or family after arrest. Furthermore, although the parent-child privilege is not as deeply imbedded in constitutional law as the attorney-client privilege, the Court determined "[the] privilege is rarely more appropriate than when a minor, under arrest for a serious crime, seeks the guidance and

29. *Id.* at 465-466.
30. 422 N.Y.S.2d 309 (Cty. Ct., Westchester Cty., 1979) (Delaney, J.).
31. *Id.* at 310 (emphasis added).
32. *Id.* at 310, 312, 313-315 (emphasis added) (internal citations omitted).
33. *Id.* at 311-312 (internal citations omitted).
34. *Id.* at 313 (citing A.&M., 403 N.Y.S.2d at 380).
35. *Id.* at 313.
36. 450 N.Y.S.2d 501 (2d Dept. 1982).

advice of a parent in the unfriendly environs of a police precinct….for such a youth, his parent is the primary source of assistance [even before a lawyer]."[37] Therefore, a youth must be provided with access to parents after arrest. In addition, applying the same measure of respect that must be accorded to attorneys and clerics,

> when [a] defendant seeks to communicate with a person and that communication would ordinarily be deemed privileged, those who hold him in custody should either (1) afford him the right to make that communication in conditions of privacy or (2) warn him that if his utterances are overheard, they may be testified to by the person overhearing them, or (3) bar all hearers from testifying to confidential communications overheard by them when conditions of privacy are not accorded and appropriate additional warnings are not given.[38]

(It should be noted, however, that the Court subsequently refused to reverse defendant's conviction based upon the erroneous admission of the privileged testimony, given the weight of the remaining evidence against the defendant, finding that the admission of such evidence was otherwise harmless. And, again, as mentioned in footnote 15, *supra*, the New York Court of Appeals, on the appeal from the Second Department in this case, declined to rule on the existence of the privilege claiming that the lack of objections at earlier proceedings failed to preserve the issue for review.[39])

Finally, in 1984 Judge Affronti, of the New York Family Court, presided over a case in which one of the issues was whether or not to expand the parent-child privilege, previously recognized by the other courts, to include communications between a defendant youth and the grandmother with whom he had lived for practically all of his life.[40] The Court ruled that the privilege does, indeed, include those people who serve in a parental capacity to the defendant.

> Even though we are not presently confronted with a parent and child, the relationship as testified to by respondent's grandmother, leads to the inference that she stands in the place and stead of his parent. To infer other wise would destroy the familial setting and self-image of the child, who should be entitled to discuss his plight without fear that his confidences will subsequently be revealed to others.[41]

In finding such a privilege, the Court concluded that the communications made while defendant suffered from remorse and guilt were shielded, since the injury to the relationship of child and [grand]parent would be much greater than the benefit to the disposal of the State's litigation.[42]

Although at this time the state of New York case law is fairly settled, it is sparse, and can result in varied outcomes depending on a case-by-case application of the law.[43] One thing is certain, however, and that is that the New York courts have created a privilege. The same cannot be said for the courts in other parts of the country, save one ruling from the United States District Court for the District of Nevada, and one from the United States District Court for the District of Connecticut (both from the *early 1980s*):

In the summer of 1982, the United States District Court for the District of Connecticut, United States District Judge Burns presiding, decided *In re Grand Jury Proceedings (Greenberg)* recognizing a limited and convoluted privilege before the Grand Jury. This grant was based solely on the religious beliefs of the mother-witness that prevented her, she argued, from either willing or forced testimony regarding incriminating information communicated to the mother by the defendant daughter.[44] This case was one of first impression in the

37. *Id.* at 504.
38. *Id.* at 505.
39. *See also* People v. Edwards, 521 N.Y.S.2d 778 (2d Dept. 1987) (citing *Harrell*, and ruling that the failure to make objections based upon parent-child privilege at earlier proceedings did not preserve the issue for review on appeal).
40. *In re Ryan,* 474 N.Y.S.2d 931 (N.Y. Fam. Ct. 1984) (Affronti, J.).
41. *Id.* at 931.
42. *Id.* at 931 (citing *Fitzgerald*, 422 N.Y.S.2d at 312 (citing Wigmore)).
43. In fact, several more recent rulings, especially at the federal level, appear to cut back on the New York privilege. *See* Clark v. Greiner, No. 97-CV-2483(JG), 2001 WL 135732 (E.D.N.Y. Feb. 2, 2001).
44. *In re Greenberg*, 11 Fed. R. Evid. Serv. (Callaghan) 579 (D. Conn. 1982) (Burns, J.).

District, and raised a number of the important issues already discussed, *supra*. The Court did not recognize a full First Amendment defense to a Grand Jury subpoena, but only a limited privilege, based on the mother's religion, where the information communicated in confidence was believed to be protected by the First Amendment.[45] Judge Burns did not, however, create or recognize a common law parent-child privilege[46] as the New York courts have done, and thus following *In re Greenberg* the parent-child privilege was not much more developed in the federal courts. Although we do not rest our proposed Privilege on a basis of religious convictions, it is important to note that *In re Greenberg* does exist, and was among the first of the federal court cases to begin placing stones into the foundation of a greater privilege.

In January of 1983, however, a very important (and so far singular) step forward was taken by then-Chief District Judge Claiborne of the United States District Court for the District of Nevada, in the landmark case of *In re Agosto*.[47] In this case, Movant sought to quash a Grand Jury subpoena, or in the alternative receive a protective order from the Court preventing his forced testimony against Movant's father. Among the arguments advanced by Movant were claims of constitutional privacy protections, as well as religious beliefs ("honor thy father and mother") protected by the First Amendment.[48] The District Court provided a very thorough and detailed decision, full of the historical roots of evidentiary privileges, and the case law of the nation both for and against the creation of new privileges - too much to review here. Much of the material is incorporated in other parts of this article. However, we should note the Court's very scholarly and convincing conclusion:

> There can be little doubt that the confidence and privacy inherent in the parent-child relationship must be protected and sedulously fostered by the courts….There is no reasonable basis for extending a testimonial privilege for confidential communications to spouses, who enjoy a dissoluble legal contract, while yet denying a parent or child the right to claim such a privilege to protect communications made within an indissoluble family unit, bounded by blood, affection, loyalty and tradition. And…if the rationale behind the privilege of a witness-spouse …serves to prevent the invasion of the harmony and privacy of the marriage…then affording the same protection to the parent-child relationship is even more compelling ….Furthermore, the parent-child relationship exhibits similarities not only to the spousal relationship…but to the psychotherapist-patient relationship, which is based upon the guidance and "listening ear" which one party…provides to the other….Open communication has a therapeutic value in the parent-child, spousal, and psychotherapist-patient settings….The family, as the basic unit of American society, is the milieu in which such values [morals, ethics, decency] are inculcated into individuals, and thus into society….If the state drives a wedge between a man and his family, the state will ultimately suffer….allowing the government to coerce testimony by parent and child against one another [will result in] individuals totally uninvolved in and innocent of the alleged wrongdoing [being] jailed for con tempt, solely because of a strong sense of family loyalty….*Indifference to personal liberty is but the precursor of the State's hostility to it*.[49]

Unfortunately, as stated earlier, most of the courts in the United States do not support a privilege for parents and children. The majority view tends to be one of favoring the plaintiff's/prosecutor's ability to gather evidence over the individual or family's right to privacy and protection from intrusion. The following few cases are presented to provide a brief review of some of the major case law and justifications opposing the creation of a family/parent-child privilege.

45. *Id.*
46. *Id.*
47. *In re Agosto*, 553 F.Supp. 1298 (D. Nev. 1983) (Claiborne, C.J.).
48. *Id*. at 1299-1300.
49. *Id.* at 1325-1331 (emphasis added) (internal citations omitted).

In 1998, the Colorado Court of Appeals handed down *People v. Agado,*[50] in which the Court affirmed the trial court's denial of parent-child privilege to statements made by the defendant to his parents regarding the crime charged. The defendant acknowledged that the Colorado Legislature had created no such privilege, but he relied upon both *Fitzgerald* and *In re Agosto* in arguing for constitutional protection, and recognition of the importance of the family unit in society. The Court was not persuaded that the defendant's rights had been trampled, and, noting that few jurisdictions had adopted the parent-child privilege, instead ruled that "[t]estimonial privileges are not lightly created nor expansively construed, for they are in derogation of the search for truth."[51]

The Massachusetts Supreme Judicial Court ruled in 1983, in *Three Juveniles v. Commonwealth*, that three children would have to appear and testify against their father, without constitutional protection for communications made within the family unit.[52] The Court followed this ruling with a somewhat different one in 2000 in *In the Matter of a Grand Jury Subpoena.*[53] In its 2000 ruling, the Court determined that it was unwilling to create a privilege at common law on the facts provided, but the Court also acknowledged the many arguments made for the creation of such a privilege. However, because the Legislature of Massachusetts had not yet acted on the matter, and because the Court recognized the importance of the issue concerning the confidential communications that had been made between the juveniles and their parents, the Court granted a stay as to the testimony sought on the confidential matters.[54] The stay was only effective until the end of the legislative session, though, and was only intended "to afford the Legislature an opportunity to address the issue…"[55] The protection granted was thus only weak and temporary, and no privilege was positively created.

Another case from the year 2000, this one in Kansas, also refused to create or recognize a common law parent-child privilege. In *Bond v. Albin*, the Court of Appeals of Kansas ruled that a father held no privilege based upon the father-son relationship that existed with his offspring.[56] In a section of the opinion comprising only a handful of sentences, the Court quickly disposed of the issue stating that Kansas statute abolished all privileges except for those expressly provided for by statute; that no Kansas statute contains a parent-child privilege; and that the father failed to present any authority that supported granting the privilege at common law based upon constitutional or statutory protections (apparently overlooking the several cases discussed earlier, including *In re Agosto*, *Fitzgerald*, and *A.&M.*).[57]

In addition to these cases from the courts of the several states, many others have also directly and indirectly dealt with the issue of parent-child privilege, and the creation of common law privileges.[58] However, space and time prevent further discussion of them here. Moreover, the many federal cases that address the issue of parent-child privilege, and subsequently deny relief, use similar justifications to those employed by the state court judges. The majority of cases, many of them Circuit cases, seem set against the creation of any common law privilege, although some of the judges seem to infer that if the factual bases of the cases were different, and the privilege sought narrowed (such as applied only to minors, etc.), perhaps the cases would have had a different result. Among the many cases that the reader might find to be of interest are: *In re The Grand Jury Empaneling of the Special Grand Jury,*[59] *United States v. Dunford,*[60] *In*

50. 964 P.2d 565 (Colo. Ct. App. 1998).
51. *Id.* at 568 (citing, among others, United States v. Davies, 768 F.2d 893 (7th Cir. 1985)).
52. 455 N.E.2d 1203 (Mass. 1983).
53. 722 N.E.2d 450 (Mass. 2000).
54. *Id.*
55. *Id.* at 457-458.
56. 28 P.3d 394 (Kan. Ct. App. 2000).
57. *Id.* at 397.
58. *See also* State v. Anderson, 28 P.3d 662 (Or. Ct. App. 2001); and In re E.F., 740 A.2d 547 (D.C. 1999).
59. 171 F.3d 826 (3d Cir. 1999).
60. 148 F.3d 385 (4th Cir. 1998).

re Grand Jury,[61] *In re Erato,*[62] *Port v. Heard,*[63] *United States v. Ismail,*[64] *United States v. Davies,*[65] and *In re Matthews.*[66]

One last case deserves mentioning because of its ruling that no parent-child or family privilege existed to prevent defendant's son from testifying against him. This was the product of *United States v. Red Elk,*[67] a 1997 decision by United States District Judge John Jones adopting the Report and Recommendation of United States Magistrate Judge Mark Moreno, both of the United States District Court for the District of South Dakota. In *Red Elk*, Magistrate Judge Moreno found that "[a]s a threshold matter, any claim of prosecutorial misconduct [before the Grand Jury], based on a violation of the 'parent-child/family' privilege must fail because there is no such privilege which defendant is entitled to assert under these circumstances."[68] Judge Moreno continued, even if a privilege existed the defendant could not invoke it, because he was seeking to block the testimony of his son. To invoke the privilege, the party asserting it must have been the one served with the *subpoena ad testificandum*.[69] Judge Moreno then rejected defendant's argument, based upon *In re Agosto*, that constitutional rights emanating from the penumbras of the Bill of Rights offer greater protection. The Court instead stated:

> Because the [*Agosto*] court quashed the subpoena prior to the child having to testify, the defendant's standing to assert the privilege never became an issue. More importantly…*Agosto* has never been followed by the Eighth [sic] Circuit and has been rejected by virtually every other federal court that has been called upon to recognize…a parent-child/family privilege.[70]

Judge Moreno concludes the discussion by ruling that even if defendant had standing to challenge the subpoena, and even if the privilege did exist, it should not have been applied in *Red Elk*. The judge found that, again, the state is entitled to "every man's evidence," there must be a great balancing of interests between the State and the defendant (and here, the scales were found to tip in favor of the State), and additionally, the crime occurred within the household, against another child in the household, preventing application of any privilege to bar the child's testimony against the father as to the accused's alleged crime.[71] Thus, the Court disavowed the existence of the privilege, and its application in the case at Bar even if it did exist.

III. The Proposed "Parent-Child Communication Privilege" and Its Parameters

We believe that a Parent-Child Confidential Communication Privilege should be created in both the federal courts and in the States, to shield parents from forced testimony (in criminal *or* civil matters) against their children[72], *and vice versa*, as to *private communications* that take place between them. Under this Privilege, both the child and the parent would have to consent before either could testify (much like the Confidential Marital Communication Privilege). The Privilege we propose, however, should not extend to non-testimonial acts that are witnessed by parents, even if those acts occur in private, and the Privilege should not apply to shield communications between parents and children that are made in public, in the presence of third-persons (including siblings who are

61. 103 F.3d 1140 (3d Cir. 1997).
62. 2 F.3d 11 (2d Cir. 1993).
63. 764 F.2d 423 (5th Cir. 1985).
64. 756 F.2d 1253 (6th Cir. 1985).
65. 768 F.2d 893 (7th Cir. 1985).
66. 714 F.2d 223 (2d Cir. 1983).
67. 955 F.Supp. 1170 (D.S.D. 1997) (Jones, D.J.; Moreno, M.J.).
68. *Id.* at 1178 (citations omitted).
69. *Id.* at 1178.
70. *Id.* at 1178 (citations omitted).
71. *Id.* at 1178-1180 (citations omitted).
72. We use the terms "child" and "children" to refer to any individual (natural, adopted or stepchild) who is still, under the laws of a particular jurisdiction, supported by parents or legal guardians. In some states, parents may be required to support a child until age 21, although the age of majority is 18. Therefore, depending on the jurisdiction, the term "child" in the Privilege may apply up until that person's 21st birthday, regardless of whether they are actually under the care and control of the parent, or regardless of whether the parents are the child's sole means of economic support (i.e. the child works to contribute to his or her own support).

not attorneys, physicians or therapists fitting the description below), or in places where there is no reasonable expectation of privacy - unless such communications are made in the presence of an Attorney, Physician, or Therapist with the express purpose of assisting in the representation, treatment, or safeguarding of the interests of the child (when the parents or guardians are acting as agents or protectors of the child). The proposed parent-child privilege should not be deemed to apply, though, to any intra-familial crimes or civil wrongs.

Both the New York spousal privilege rule and the Idaho Code provide language that could be modified and adapted in a new Model Parent-Child Privilege to better protect the liberty interests and privacy of defendants and party-witnesses.

> New York:
> (b) Confidential communication privileged. A husband or wife shall not be required, or, without consent of the other if living, allowed, to disclose a confidential communication made by one to the other during marriage.[73]

> Idaho:
> (7) Any parent, guardian or legal custodian shall not be forced to disclose any communication made by their minor child or ward to them concerning matters in any civil or criminal action to which such child or ward is a party. Such matters shall be privileged and protected against disclosure; excepting, this section does not apply to a civil action or proceeding by one against the other not to a criminal action or proceeding for a crime committed by violence of one against the person of the other, nor does this section apply to any case of physical injury to a minor child where the injury has been caused as a result of physical abuse or neglect by one or both of the parents, guardian or legal custodian.[74]

When considering whether to create a new privilege by common law, courts must consider several different tests. The Third Circuit has reasoned, "Congress manifested an affirmative intention not to freeze the law of privilege [under Rule 501]. Its purpose rather was to 'provide the courts with the flexibility to develop rules of privilege on a case-by-case basis'…and leave the door open to change."[75] Of course, the Court goes on to assert that any recognition of a new privilege must overcome the centuries old tradition of the state's entitlement to the evidence of every man,[76] and the law's heavy dependence on receiving all existing evidence.[77] According to the Supreme Court in Trammel, Federal Rule 501 "requires that the court engage in a balancing process, weighing the need for confidentiality in a particular communication against the need for relevant evidence in a criminal proceeding."[78] However, Judge Mansmann goes on to also reference Wigmore's four-part test for determining when to recognize a new privilege. For privilege to attach, Dean Wigmore stated that:

> (1) the communications must originate in a confidence that they will not be disclosed; (2) this element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties; (3) the relation must be one which, in the opinion of society, ought to be sedulously fostered; and (4) the injury that would inure to the relation by the disclosure of the communication must be greater than the benefit thereby gained for the correct disposal of litigation.[79]

Given the justifications contained in the opinions of the New York Courts (especially the Fourth Department in *A.&M.*), *supra*, and the great societal concerns and rationales expressed herein and in the cited

73. N.Y. C.P.L.R. 4502(b) (McKinney 2002).

74. IDAHO CODE § 9-203(7) (Michie 2003). Note that the language quoted from New York and Idaho is similar to the privilege provisions proposed in this article, but that some language has been altered, and several other important provisions have been changed, added or deleted accordingly.

75. Pearson v. Miller, 211 F.3d 57, 66-67 (citing, among others, *Congressional Record* entries).

76. *See In re Greenberg*, 11 Fed. R. Evid. Serv. (Callaghan) 579 (D. Conn. 1982) (citing *In re Cueto*, 554 F.2d 14, 15 (2d Cir. 1977)).

77. Pearson, 211 F.3d at 67 (internal citations omitted).

78. *In re Grand Jury*, 103 F.3d 1140, 1159 (3d Cir. 1997) (Mansmann, J., concurring & dissenting) (citing Trammel v. United States, 445 U.S. 40, 50 (1980)).

79. 103 F.3d at 1160 n.5 (citing 8 John Henry Wigmore, *Evidence* § 2285 (J. McNaughton rev. ed. 1961); and *In re* Grand Jury Investigation, 918 F.2d 374, 383-84 (3d Cir. 1990)); and 403 N.Y.S.2d at 381. Note the similarity between Dean Wigmore's fourth prong and the *Trammel* Court's balancing test.

authorities, we believe that the Parent-Child Privilege that we have proposed could more than likely survive the *Trammel* and Wigmore tests, and become an integral part of the law of evidence. In fact, when rendering its decision, the Court in *Fitzgerald* applied Wigmore's test, and concluded in that particular case and under those facts that the test *was* met.[80]

First, as has been said by one learned jurist, to force parents to testify against children, or reveal confidences disclosed to them "is inconsistent with the way of life we cherish and guard…and raises the specter of a regime which encourages betrayal of one's offspring. And…the alternatives faced by the parents, i.e., risk of prosecution for contempt or commission of perjury, *could seriously undermine public trust in our system of justice*."[81] The same could be said of forcing children to so testify against their parents. At specific times in history, regimes have used similar tactics to secure State convictions of defendants. The reader is familiar with the memory of those undemocratic regimes, including Nazi Germany and the former Soviet Union. "We know that one of the horrors of Nazi Germany was children snitching on their parents. It seems to me common decency that you don't put a child before the grand jury on her mother's conduct."[82] Truly, how beneficial can it be for the mental and emotional development of a child, and for the integrity of the family, if children are required to testify against parents?[83] Therefore, we recommend that the privilege go both ways, and prevent parents from being forced to testify against children and children from being forced to testify against parents concerning things discussed in the household - in the interest of fortifying and elevating the level of privacy, unity and liberty enjoyed by the American family unit.[84] Indeed, Professor Watts may have stated it best when she wrote:

> …parent-child privileges, and the testimonial privileges in general, are conspicuously absent in totalitarian regimes. Nazi Germany had no such privileges….Without adoption of a parent-child privilege in the United States, we face a similar intrusion into the privacy of the family….it is important that we prevent any further harm to the individual's integrity and the family's autonomy.[85]

Although Professor Watts wrote this over a decade and a half ago, nothing more has been accomplished by the courts and legislatures in the way of creating a parent-child privilege. It is time to reawaken the public and the justice system with regard to the need for this privilege, especially at this time when we must be ever vigilant to guard individual and family liberty and privacy interests against intrusion by government agents who may be seeking to encroach on them under the guise of combating terrorism. Must we continue to offer little more protection for the family unit, and confidences expressed therein, than did the Soviets and Nazis?[86] The slow uptake by most courts and legislatures on this point is truly perplexing in its perseverance.

Many European nations, including Sweden, Germany (the former West Germany), and France have very strict familial privileges - which spring from both the *Corpus Juris Civilis* (Roman Body of Civil Law) and the Napoleonic Code of old

80. 422 N.Y.S.2d 309, 312 (Cty. Ct., Westchester Cty., 1979).

81. 403 N.Y.S.2d at 380 (emphasis added).

82. Watts, *supra* note 1, at 583 (quoting Burke, *Nevada Girl, 16, Ordered to Testify Against Mother*, NAT'L L.J., Mar. 9, 1981, at 3, col. 2 (quoting Irving Younger)).

83. "Our cases make clear that an asserted privilege must also 'serve public ends'….The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance." Jaffee v. Redmond, 518 U.S. 1, 11 (1996) (citing, among others, Upjohn Co. v. United States, 449 U.S. 383, 389 (1981); and United States v. Nixon, 418 U.S. 683, 705 (1974)).

84. "A son feels, perhaps, even a greater duty to listen to the confidences of his father, in that his perceptions of himself as his father's confidante is a powerful step in the growth process and the feeling of mutuality and respect within the relationship….It can even be argued that there is a role reversal in the parent-child relationship, as the parent grows older and becomes more reliant on the child. In this regard, the parent becomes a child…and the child assumes the role of parent and protector…." *In re Agosto*, 553 F.Supp. 1298, 1329 (D. Nev. 1983).

85. Watts, *supra* note 1, at 593-594.

86. See *In re Agosto*, 553 F.Supp. 1298, 1302 (D. Nev. 1983), for a discussion of a litigant's argument that a family privilege ought to be created to avoid the resurrection of a "Hitlerian" society "in which the right of privacy, inherent in the family unit, is completely ignored where it is deemed inconsistent with the state's purposes."

- and which often extend far beyond even the model U.S. rules to include grandparents, in-laws and even spouses post-divorce.[87] All in all, Professor Watts claims that the idea of a parent-child or familial privilege has been in existence for 3,500 years or more! The Books of Moses (the first five books of the *Bible*, or Pentateuch), and the subsequent development of the Judaic common law, contain provisions forbidding parents to testify against children, and other prescriptions for family unity.[88] But perhaps the best story of all is one that poignantly illustrates how the creation and preservation of a strong privilege law is for the good of the many, and therefore the good of the few (in *this* case, the government or civil plaintiff) must bow to it. As Professor Watts relates it, the great Roman orator and philosopher Cicero was prosecuting the Roman Governor of Sicily for bribery. The Roman Civil Law contained a provision known as *testimonium domesticum* (a parent-child, or domestic, testimonial privilege). Cicero was therefore prevented from calling the Governor's patronus (father or father-figure) to testify against the Governor at trial. Instead of lamenting the restriction on the prosecution, or heatedly seeking legislative appeal, Cicero instead "regretted not being able to call the patronus but understood *and advocated the potential social policy considerations* for the exclusions of the testimony."[89] After all, Cicero himself said, "The good of the people is the greatest law."[90]

Moreover, in many states, such as New York, parents are responsible for the support (especially financial support) of their children until ages 18 or 21, depending upon the jurisdiction. It is not reasonable to expect parents to fully and effectively exercise their responsibilities if children cannot freely confide in their parents regarding any concerns, issues, or even improper or illegal actions, without fear that their parents will then become the star witnesses against them at a later civil or criminal proceeding. Today, we hear a lot about the decline of "family values" and the need to reestablish and secure "family values." In reality, parents are, and should be, the first people children will turn to when a serious event has occurred in their lives. If a child commits a crime, or is involved in a civil legal problem, they are very likely to be confused and frightened - just as if they were victims of a crime or civil wrong.[91] Parents can be a source of advice, guidance, and consolation. That role, however, can be chilled if one part of their mind is waiting for the prosecutor or process-server to ring the doorbell and subpoena their testimony.

Furthermore, spouses, depending on the jurisdiction, receive testimonial privileges (either Spousal Immunity or Confidential Marital Communication, or both).[92] This is because society through its legislatures and courts, has determined that it is of the utmost importance to shield a marriage, and

87. Watts, *supra* note 1, at 593 (citing and quoting, among others, Article 248 of the French Civil Code). *See also In re Agosto*, 553 F.Supp. at 1306, for a discussion of the Roman *testimonium domesticum*, and its application.

88. Watts, *supra* note 1, at 591-592.

89. *Id.* at 592-593 (emphasis added).

90. *De Legibus*, bk. 3, ch. 3, § 8, *quoted in* THE COLUMBIA DICTIONARY OF QUOTATIONS 507 (1993).

91. *See* Ayala & Martyn, *supra* note 5, at 179 ("[W]hen children are faced with a serious problem and are unsure about how to handle themselves, their first reaction is usually to seek assistance and advice from their parents. Because children are inclined to confide in their parents, there exists a need for the free flow of highly personal information.").

92. The Federal courts grant spouses both the Confidential Marital Communications Privilege and Spousal Immunity Privilege, except that while both party and witness-spouse hold the privilege when it comes to communications, the privilege lies only in the witness-spouse when the Spousal Immunity privilege is involved. Trammel v. United States, 445 U.S. 40 (1980). In contrast, New York has a much narrower privilege for spouses, providing for a very limited ability for spouses to testify in adultery cases, and recognizing only the Confidential Communication Privilege - a privilege that protects only confidential communications, not acts, made between spouses *during* the marriage. *See* N.Y. C.P.L.R. 4502 (McKinney 2002); *In re Donald Sheldon & Co., Inc.*, 191 B.R. 39, 47 (Bankr. S.D.N.Y. 1996) (citing People v. McCormack, 104 N.Y.S.2d 139, 143 (1st Dept. 1951), for the existence of the marital communication privilege in New York). However, in New York, the communication privilege is not applicable in all circumstances, such as when frauds are being perpetrated under the cover of the marital privilege. The communication must be one that would not otherwise have been made "but for the absolute confidence in, and induced by, the marital relationship." *In re Sheldon*, 191 B.R. at 47-48 (citing People v. Melski, 176 N.E.2d 81 (N.Y. 1961)). We model our proposed Parent-Child Confidential Communication Privilege largely after both the New York spousal privilege and IDAHO CODE § 9-203(7) (Michie 2003), *supra*.

not interfere with the private relationship that exists between a husband and wife in the "marital castle." Just as the need for encouraging "full and frank communication between attorneys and their clients" to promote greater justice and protection of individual liberty justifies the attorney-client privilege, so too "the spousal privilege, as modified in *Trammel*, is justified because it 'furthers the important public interest in marital harmony.'"[93] But, what about society's children? Children are related to parents by *blood* (or in the case of adoption, by a legal order that creates a link as if by blood).[94] This relationship is, and should be, just as important as marriage to the well-being of the citizenry - at least to the limited extent of the Privilege outlined above. Much like the justification for the Attorney-Client Privilege, children must have the ability to openly communicate with their parents in an environment free from the fear that they will be exposing themselves to adverse testimony by parents, and to better facilitate their access to parental advice, guidance, and protection.[95]

Indeed, given the current state of affairs in the clergy of some religions, and the turbulent nature of our world in general, it makes no sense to continue to insist that the clergy-penitent privilege be enforced between two strangers united only in faith, or that the attorney-client privilege be enforced between two strangers united only in business, or that the physician-patient privilege be enforced between two strangers united only in treatment (or insurance coverage), and yet not insist, with outrage at their apathy, that the legislators in Congress and the states at once create a parent-child privilege to protect those confidences and communications made in the privacy of what should be that most sacred of institutions in our nation - the family unit.

Considering all of the arguments and justifications, it would appear that the Parent-Child Privilege model proposed herein would meet the four-prong test set out by Wigmore and the balancing test of the *Trammel* Court for the creation of a new privilege in evidence law.[96]

IV. Conclusion

We are left with a very uncertain and unsettled area of law that impacts on the lives of civil and criminal defendants, and could potentially touch the lives of many, many more. For this reason, we have addressed the issue of creating a Parent-Child Privilege head-on, and we encourage Congress and the Legislatures and High Courts of the several states to consider such a privilege. This Privilege, if created, would greatly strengthen the justice system, the institution of the family, and the existence of family values in America. Given the clear and compelling justifications outlined above, reading the persuasive opinions of those progressive Courts that have begun to construct the foundation of a familial privilege in the law, and considering the important role that a Parent-Child Communication Privilege would play in the American Justice System, we see no other justifiable position to take on this issue.

The Pax Romana may exist no longer, but the Privata Lex should remain viable in the interests of preserving family values.

---

93. Jaffee v. Redmond, 518 U.S. 1, 11 (citing Trammel, 445 U.S. at 53; United States v. Nixon, 418 U.S. 683, 705 (1974); and Wolfle v. United States, 291 U.S. 7, 14 (1934)).

94. *See also In re Agosto*, 553 F.Supp. 1298, 1325 (D. Nev. 1983).

95. Attorney-Client Privilege and Confidentiality "…have been designed to assure that clients can speak openly with their attorneys, secure in the knowledge that they cannot be harmed by words spoken or any incriminating facts disclosed to attorneys when legal assistance is sought. 'This, in turn, will result in more informed legal advice…' It is hoped that, as a result, clients will be more forthcoming with information to their attorneys, allowing lawyers to better advise…clients." Michael L. Fox, Note, *To Tell or Not to Tell: Legal Ethics and Disclosure After Enron*, 2002 COLUM. BUS. L. REV. 867, 900-901 (2002) (Part of Survey, *Breaking Rocky Ground: Issues in Investment and Ethics in a Shaken Economy*, 2002 COLUM. BUS. L. REV. 793 (2002)), (citing, among other sources, Paul R. Rice, *The Corporate Attorney-Client Privilege: Loss of Predictability Does Not Justify Crying Wolfinbarger*, 55 BUS. LAW. 735, 739 (2000)).

96. See pages 51-52 & nn.78-80, *supra*.

The Privacy Project II

The Deliberative Process Privilege: What is it? When can it be asserted? How can this shield be pierced?

By Cathy Havener Greer, William T. O'Connell and Kirsten J. Crawford

In the post-Watergate era, "transparency" became a watchword of government. Freedom of information, open records, open meetings are considered by the media and to some extent, the public, the standards by which government should exercise its responsibilities. In spite of the desire of the media and the public for totally open government, the deliberative process privilege protects government officials and government documents from "full disclosure."

The Deliberative Process Privilege is a widely-recognized confidentiality privilege that is unique to the government. *See Coastal States Gas Corp. v. Dept. of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980). This privilege in the United States is thought to have derived from the "crown privilege" in England. *See* Russell L. Weaver and James T. Jones, *The Deliberative Process Privilege*, 54 MO. L. REV. 279, 283 (1989).

Two primary theories form the justification for the privilege: First, in order to maintain the integrity of administrative processes, decisions made by agency administrators should be protected from discovery in the same way that the decision-making processes of judges are protected; and second, in order to maintain frank and open exchange of opinions and recommendations between government officials, consultation between such officials and the government's decision makers should be protected from disclosure. See *McGoldrick v. Koch*, 110 F.R.D. 153, 155 (S.D.N.Y. 1986); *Morgan v. United States*, 304 U.S. 1, 18, 58 S.Ct. 773, 82 L.Ed. 1129 (1938) (Morgan I); *United States v. Morgan*, 313 U.S. 409, 422, 61 S.Ct. 999, 1004, 85 L.Ed.2d 1429 (1941) (Morgan II); *Capital Info. Group v. Alaska*, 923 P.2d 29, 33 (Alaska 1996); *Colorado Springs v. White*, 967 P.2d 1042, 1047 (Colo. 1998).

Although the privilege is recognized to have a constitutional and common law basis, both federal and state legislators have incorporated this privilege into exceptions to freedom of information and open records laws. In addition, a number of state courts have recognized this privilege. *See, e.g., Capital Info. Group v. Alaska, supra; Times Mirror Co. v. Superior Court*, 53 Cal.3d 1325, 283 Cal. Rptr. 893, 813 P.2d 240, 248-51 (Cal. 1991); *Hamilton v. Verdow*, 287 Md. 544, 414 A.2d 914, 924 (Md. 1980; *Ostoin v. Waterford Township Police Dep't*, 189 Mich. App. 334, 471 N.W.2d 666, 668 (Mich. Ct. App. 1991); *Nero v. Hyland*, 76 N.J. 213, 386 A.2d 846, 853 (N.J. 1978); *State ex rel. Attorney Gen. v.*

IADC member Cathy Havener Greer is a member of Wells, Anderson & Race LLC, of Denver, where her practice emphasizes employment and civil rights litigation. She is a graduate of Randolph-Macon Woman's College (B.A. 1973) and the University of Kansas School of Law (J.D. 1976).

William T. O'Connell is an associate at Wells, Anderson & Race LLC, where his practice emphasizes employment and civil rights litigation. He graduated from Norwich University (B.S. 1992) and Suffolk University Law School (J.D. 1997).

Kirsten J. Crawford, formerly an associate of Wells, Anderson & Race, LLC, is now an Assistant County Attorney, Adams County, Colorado. She is a graduate of DePauw University (B.A. 1993) and the University of Denver (J.D. 1996).

First Judicial Dist. Court, 96 N.M. 254, 629 P.2d 330, 333-34 (N.M. 1981); *Dorchester Master Ltd. Partnership v. Cabot Pipeline Corp.*, 137 Misc.2d 442, 521 N.Y.S.2d 209, 210-11 (N.Y.Sup.Ct. 1987); *Killington, Ltd. v. Lash*, 153 Vt. 628, 572 A.2d 1368, 1373-74 (Vt. 1990). *See also* 5 U.S.C. § 552(b)(5), Federal Freedom of Information Act (FOIA).

In Morgan II, 313 U.S. 409 at 421-422, the United States Supreme Court decisively confirmed the justification for the deliberative process privilege. Criticizing the district court's authorization of the deposition of the U.S. Secretary of Agriculture, Justice Frankfurther, writing for the majority, said

> . . . [T]he short of the business is that the Secretary should never have been subjected to this examination. The proceeding before the Secretary 'has a quality resembling that of a judicial proceeding'. Morgan v. United States, 298 U.S. 468, 480, 56 S.Ct. 906, 911, 80 L.Ed. 1288. Such an examination of a judge would be destructive of judicial responsibility. We have explicitly held in this very litigation that 'it was not the function of the court to probe the mental processes of the Secretary'. 304 U.S. 1, 18, 58 S.Ct. 773, 776, 82 L.Ed. 1129. Just as a judge can not be subjected to such a scrutiny, compare Fayerweather v. Ritch, 195 U.S. 276, 306, 307, 25 S.Ct. 58, 67, 49 L.Ed. 193, so the integrity of the administrative process must be equally respected. See Chicago, B. & Q. Ry. v. Babcock, 204 U.S. 585, 593, 27 S.Ct. 326, 327, 51 L.Ed. 636. It will bear repeating that although the administrative process has had a different development and pursues somewhat different ways from those of courts, they are to be deemed collaborative instrumentalities of justice and the appropriate independence of each should be respected by the other. United States v. Morgan, 307 U.S. 183, 191, 59 S.Ct. 795, 799, 83 L.Ed. 1211.

This privilege, which has been cited under the names of "administrative deliberative thought process privilege," "official information privilege," "governmental privilege," "executive privilege" and "deliberative process privilege," is asserted to protect documents from disclosure and to protect a witness from providing testimony at a deposition or trial. The context in which the privilege may be raised is very broad: from an inquiry into the basis for a quasi-judicial decision such as a zoning appeal or personnel grievance hearing, to an executive decision including "advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated." *Carl Zeiss Stiftung, et al. v. V.E.B. Carl Zeiss Jena, et al.*, 40 F.R.D. 318, 324 (D.D.C. 1966).

Significantly, the privilege applies not only to the process of the decision maker in reaching his decision, but to the advice given to the decision maker. *Carl Zeiss Stiftung v. V.E.B. Carl Zeiss, Jena*, 40 F.R.D. 318 (D.D.C. 1966). As the District Court judge in Carl Zeiss Stiftung stated:

> The judiciary, the courts declare, is not authorized 'to probe the mental processes' of an executive or administrative officer. [*] This salutary rule forecloses investigation into the methods by which a decision is reached, [*] the contributing influences, [*] or the role played of the work of others, [*] - results demanded by exigencies of the most imperative character. No judge could tolerate an inquisition into the elements comprising his decision [*]--indeed, '[s]uch an examination of a judge would be destructive of judicial responsibility' [*] --and by the same token 'the integrity of the administrative process must be equally respected.' [*] Identically potent reasons dictate that protection no less extensive be afforded the processes by which the Attorney General's responsibilities for decisional and policy formulations, legal or otherwise, are dis charged. [*] (footnotes omitted)

Id. at 325-26. The court in *Carl Zeiss* also noted:

> Inextricably intertwined, both in purpose and objective, are these two principles. The rule immunizing intra-governmental advice safeguards free expression by eliminating the possibility of outside examination as an inhibiting factor, but expressions assisting the reaching of a decision are part of the decision-making process. [*] Similarly, the so-called 'mental process rule' impresses the stamp of secrecy more directly upon the decision than upon the advice, but it extends to all phases of the decision- making

> process, of which the advice is a part. [*] Each rule complements the other, and in combination they operate to preserve the integrity of the deliberative process itself. It is evident that to demand pre-decision data is at once to probe and imperil that process. (footnotes omitted)

Subsequent case law further refined the privilege. *See Kaiser Aluminum & Chemical Corp. v. United States*, 141 Ct. Cl. 38, 157 F.Supp. 939 (Ct. Cl. 1958); *In re Sealted Case*, 121 F.3d 729, 736 and 742 (D.C. Cir. 1997). The deliberative process privilege is a qualified, not absolute, privilege. Because its purpose is to prevent inquiry or disclosure that would undermine the free exchange of ideas within an agency or would inhibit the integrity of the decision-making process, it protects only information that is predecisional and deliberative. *Id.* at 737.

Recent Cases in Which Deliberative Process Privilege Found Applicable

Although recent cases which have applied the deliberative process privilege lack a common theme, it is likely that the "deliberative" element of the privilege, more so than the predecisional element, will command the court's attention. The reason for this attention stems from the fact that the predecisional element is often easier to establish and more given to a bright line test. In contrast, the deliberative element usually requires a more careful and thorough analysis of the nature of the communication itself, the participants in the communication and the underlying events which precipitated the communication.

In *Jones v. City of Indianapolis*, 216 F.R.D. 440 (S.D. IN 2003), plaintiff, the mother of an arrestee who died on the way to a hospital in an Indianapolis Police Department paddy wagon, filed suit under 42 U.S.C. 1983 against the City of Indianapolis and several individual police officers. During discovery, plaintiff served a document request seeking production of certain document including those generated during the Police Department's internal investigation of the incident. *Id.* at 443. Defendants objected on the basis that the requested documents were "official, confidential, deliberative, and/or investigatory in nature and thus are privileged from discovery." *Id.*

The court held that the deliberative element of the privilege had been met for three primary reasons. First, the Police Department's "deliberations" were of a continuing nature as evidenced by the Police Department placing the individual officers involved in the incident on administrative leave. Id. Second, the United States Department of Justice had begun its own investigation which could lead to criminal indictments. *Id.* Finally, the Police Department could still issue further disciplinary action against the individual officers. *Id.*

In *Yankee Atomic Electric Company v. United States*, 54 Fed. Cl. 306 (Fed. Claims 2002), plaintiffs, various electric utilities, filed suit against the United States for breach of contract relating to the disposal of nuclear waste. Defendant asserted the deliberative process privilege over a number of documents described in an affidavit from the Chief Operating Officer, Civilian Radioactive Waste Management, within the United States Department of Energy.[1] Plaintiffs argued that the documents at issue were not privileged because they were incorporated into an official agency decision. *Id.* at 311.

The court found Plaintiffs' argument unpersuasive because the documents described in the affidavit appeared to be non-binding recommendations; were not, as best as the court could determine, final dispositions; were not used as precedent; had no operational effect except to the extent they informed agency officials; and were not expressly incorporated into or adopted by final agency decision. *Id.* Similarly, the

1. A secondary issue in the case was whether the head of the agency, the Secretary of Energy, had to personally invoke the privilege. The court found no such requirement in order to invoke the privilege and further found that the Secretary of Energy was not prohibited from delegating the power to invoke the privilege. *Id.* at 311. The proper way to invoke the privilege will be discussed more fully below.

court found no merit to Plaintiffs' argument that the privilege was negated by defendant's failure to identify a specific agency decision that was later based on the documents at issue. *Id.* at 312. The court observed that the affidavit provided sufficient information with which to conclude that the document was prepared in order to offer opinions or recommendations to agency decision makers prior to their taking action on legal or policy matters. *Id.*

In *Capital Information Group v. State of Alaska*, 923 P.2d 29 (Alaska 1996), the issue before the Alaska Supreme Court was whether the deliberative process privilege applied to legislative proposals sent from state departments and agencies directly to the Governor and/or budget memoranda sent from each state department to the Alaska Office of Management and Budget ("OMB"). With respect to the legislative proposals, the court recognized that they were clearly predecisional and deliberative. *Id.* at 37. With those two initial elements satisfied, the court turned to whether the privilege should be overcome by weighing the "interest of the citizen in knowing what the servants of government are doing ... against the interest of the public in having the business of government carried on efficiently and without undue interference." *Id.* at 38 (internal citations omitted). In holding that the privilege was not overcome, the court found that the consideration of legislative proposals "is one of the most sensitive and important functions that the Governor performs while in office, and the need for frank discussion of policy matters among the Governor's advisors is perhaps greater here than in any other area." *Id*. at 38.

The court likewise found that the budget memoranda was both predecisional and deliberative. *Id.* at 39. However, unlike the legislative proposals, the court held that the weighing of interests compelled disclosure of the documents. *Id.* at 39-40. In reaching its determination, the court relied on a state statute, AS 37.07.050, which mandates that such budget documentation be made and submitted to OMB. *Id.* at 40. *Id*. Accordingly, the court held that the deliberative process privilege did not apply to the memoranda. *Id.*

Not all cases applying the deliberative process privilege involve highly sensitive and significant materials like the internal investigation documents at issue in Jones or the legislative proposals at issue in *Capital Information Group*. Rather, some cases deal with seemingly mundane materials. Nevertheless, a challenge to the disclosure of the documents pursuant to the deliberative process privilege may still prove successful.

In *Tribune-Review Publishing Company v. Dep't of Community and Economic Development*, 814 A.2d 1261 (Pa.Cmwlth. 2003), the issue before the Commonwealth Court of Pennsylvania was whether unfunded state program applications were public records subject to disclosure pursuant to Pennsylvania's Right to Know Act. The court held that the unfunded applications were part of the deliberative process and therefore not subject to disclosure under the Act. *Id.* at 1264. The court found that the unfunded applications reflected the "administrative machinations" of the state with respect to which grants to fund or not to fund. *Id.* "Absent a showing that an agency has acted upon the applications, i.e., done more than merely characterize, we conclude that the mere characterization of grant applications as 'unfunded' reflects the deliberative process and as such the documents are not subject to disclosure." *Id*. The court also found significant the fact that there was no evidence that the documents at issue formed either the basis for, or a condition precedent of, the state's decision to fund the applications. *Id.* As such, the court determined that the documents were not essential components of an agency decision. *Id.* at 1264. The court cautioned, however, that once the applications are acted upon, i.e., granted, than they are public records subject to disclosure. *Id.*

The protection for predecisional and deliberative matters remains after the decision is made, although it does not apply to the publicly expressed reasoning of the

decision maker underlying the decision itself. *Id.*, 967 P.2d at 1051-52.

In a deposition or in anticipation of a deposition seeking disclosure of documents reflecting predecisional thought processes and advice, the assertion of the privilege is made properly in an objection or motion for protective order. In an action under the Colorado Open Records Act, "[t]he initial burden of proof falls upon the government entity asserting the deliberative process privilege." *Colorado Springs v. White*, 967 P.2d at 1053 [citations omitted]. "Where the government has met the procedural requirements [of the Colorado Open Records Act] for assertion of the deliberative process privilege, the privilege presumptively applies." *Id.*, 967 P.2d at 1054 [citations omitted]. The procedural requirements for assertion of the privilege are set out in § 24-72-204 (3)(a)(XII), cited above.

Even in the Open Records context, where a presumption favoring disclosure is the general rule, "a trial court should honor the claim of privilege unless the party seeking discovery makes a preliminary showing that the material may not be privileged or that there is some necessity for its production. See *Guy v. Judicial Nominating Com'n*, 659 A.2d 777, 785-86 (Del. Super. Ct. 1995) (noting that the executive privilege protects from disclosure both the source of and the substance of communications to and from governor in exercising his power of appointment of judges, and declining to conduct an *in camera* inspection because plaintiff had not meet his burden to overcome the presumption of protection; also ruling that allegations that information was "leaked" did not constitute a waiver by the governor, as the privilege is his only to waive, and that allegations of discriminatory treatment did not state any claim under the Delaware open records law); *Hamilton v. Verdow*, 414 A.2d 914, 925 (Md. App. 1980).

If a decision maker is allowed to testify, that person's testimony concerning the decision must be circumscribed. "When pertinent inquiry is allowed, it is limited to information concerning the *procedural steps* that may be required by law and does not extend to inquiries into the mental processes of an administrator, which, as being part of the judgmental process, are not discoverable." *State of Iowa ex rel. Miller v. DeCoster*, 608 N.W.2d 785 (Iowa. 2000).

Proper Way to Invoke the Privilege

The method a party uses to invoke the privilege must be scrutinized because failure to properly invoke it will likely result in the court's refusal to rule on the applicability of the privilege.

In *Cobell v. Norton*, 213 F.R.D. 1 (D.C. 2003), the issue before the court was whether a document filed by the government defendants under seal was protected pursuant to the deliberative process privilege. The court, however, declined to rule on the issue because the defendants had not properly invoked the privilege. *Id*. at 7.

The court observed that in the D.C. Circuit, the proper invocation of the privilege requires:

> (1) a formal claim of privilege by the head of the department possessing control over the requested information, (2) an assertion of the privilege based on actual personal consideration by that official, and (3) a detailed specification of the information for which the privilege is claimed, along with an explanation why it properly falls within the scope of the privilege. *Id*. at 7 citing *Landry v. FDIC*, 204 F.3d 1125, 1135 (D.C.Cir.2000).

Although the court declined to discuss the contents of the document and consequently the precise reason for finding that defendants did not properly invoke the privilege, one can derive where the defect lay given the court's focus on the first element of the three element test. The court noted that in the D.C. Circuit, the term "head of the agency" has not been narrowly construed. *Id.* at 8. (citations omitted). Nevertheless, the court cautioned that while it was unnecessary for the Secretary of the Interior herself to file an affidavit in order to assert the deliberative process privilege, the head of the bureau or office within the Interior Department that possesses control

over the requested information must file the necessary affidavit. *Id.* at 8.

Recent Cases in Which Deliberative Process Privilege Found Inapplicable

A recurring theme throughout the recent cases in which the deliberative process privilege has been found inapplicable is the court's reluctance to apply the privilege when faced with allegations of discrimination and/or retaliation. In light of the qualified nature of the deliberative process privilege, allegations of this sort may implicate the government misconduct exception to the privilege. Of course as employment lawyers are well aware, in any case in which a plaintiff alleges discriminatory conduct by a defendant, the defendant must present "a legitimate nondiscriminatory reason" for the employment action at issue or face an adverse judgment. For that reason, in the face of discrimination allegations, a government employer that asserts deliberative process privilege does so at its peril.

In *Chaplaincy of Full Gospel Churches v. Johnson*, 2003 WL 22048206 (D.D.C. 2003), plaintiffs, current and former Navy chaplains, filed suit against the Navy, the Secretary of the Navy and other Navy officials claiming that the Navy's polices and practices favored religious quotas and other discriminatory practices in violation of the First and Fifth Amendments. During discovery, Plaintiffs sought the deposition testimony of navy chaplain selection board personnel. *Id* at *2. Defendants refused based in part on the deliberative process privilege. *Id*.

With respect to the government misconduct exception to the privilege, the court noted "[w]hen there is any reason to believe that government misconduct has occurred...our court of appeals has made clear that the deliberative-process privilege disappears altogether." *Id*. (citations omitted). To invoke the government misconduct exception, the party seeking the discovery "must provide an adequate factual basis for believing that the requested discovery would shed light upon government misconduct." *Id.* The plaintiffs pointed to various reports and statistics which plaintiffs claimed raised questions about the impartiality of the chaplain selection boards. *Id.* at * 6. The court found that Plaintiffs had provided the requisite factual basis, through these reports and statistics, for their belief that the testimony of navy chaplain selection board personnel would provide evidence of government misconduct. *Id*. at *6. Accordingly, the court held that the government-misconduct exception barred application of the deliberative-process privilege.

In *Williams v. City of Boston*, 213 F.R.D. 99 (D. MA 2003), plaintiff, a Boston police officer, brought a civil rights action against defendants alleging discrimination and retaliation. In response to Plaintiff's request for production of documents, defendants refused to produce, pursuant to the governmental/deliberative process privilege, the reports of hearing officers who conducted disciplinary hearings relating to two of the individual defendant police officers. *Id.* at 100. Defendants contended that the reports were privileged because they reflected "advisory opinions, recommendations and deliberations comprising part of the process by which governmental decisions and policies are formulated." *Id.*

The court held the governmental or deliberative process privilege inapplicable to the reports. "The hearing officers' recommendations, like the facts which are contained in the Reports, is information passed on to the Commissioner for his consideration. It is not supposed to form the subject of discussion between the hearing officer and the Commissioner, and its production should in no way chill the Commissioner's decision-making process..." *Id*. at 101. Accordingly, the court found that disclosure of the reports would in no way interfere with the decision-making process that the privilege is designed to protect. *Id*. at 102. Significantly, the court also recognized that the privilege is particularly disfavored in civil rights cases, especially those against police departments. *Id.* at 102 citing *Soto v. City of Concord*, 162 F.R.D. 603, 612 (N.D.

Cal. 1995)(finding deliberative process privilege "inappropriate for use in civil rights cases against police departments"). Finally, the court noted in conclusion that where the " 'decision-making process itself is the subject of the litigation,'" application of the deliberative process privilege is inappropriate since it would act to preclude discovery of relevant information. *Id*.

In *Waters v. U.S. Capitol Police Board*, 216 F.R.D. 153 (D. D.C. 2003), plaintiff, a recruit terminated from U.S. Capitol Police for cheating on a written examination, brought a Title VII race discrimination action. During discovery, Plaintiff sought the production of a written report generated during the investigation into his alleged cheating as well as documents generated during a second investigation into his claim of discrimination. *Id.* at 161. With respect to the first request, Defendants objected and withheld a memorandum from a Police Captain to the Assistant Chief. Id. With respect to the second request, defendants produced all documents with the exception of the notes made by the officer responsible for investigating plaintiff's discrimination claims. *Id.* at 162.

Turning first to the investigators' notes, the court held that they were not protected by the deliberative process privilege. The court found significant the fact that the notes were not claimed to constitute "'opinions, recommendations and deliberations' that must be shielded lest inferiors in a government agency be inhibited in the advice they give their superiors or the public will be misled as to the reasons for the ultimate adoption of a particular policy.' " *Id* at 162 citing *Taxation with Representation Fund v. Internal Revenue Service*, 646 F.2d 666, 677 (D.C.Cir.1981). The court also observed that defendants were not claiming that the notes were created by individuals who had the responsibility of recommending the adoption of a particular policy by the U.S. Capitol Police. *Id.*

With respect to the memorandum, the court likewise found that it was not protected by the deliberative process privilege. The court was persuaded by the fact that this was not a situation where the Assistant Chief was considering a policy and sought the Captain's views on same or a situation where the Captain was proposing a policy for the Assistant Chief to adopt. *Id.* at 162. The court instead viewed the memorandum as one in which the Captain was simply speaking to a lone, particular case. *Id.* at 163. Moreover, the court noted that the memorandum could implicate the issue of intent to discriminate or retaliate since the memorandum related to the investigation of plaintiff's alleged cheating and plaintiff's primary claim was that the investigator in charge of such investigation discriminated him because of his race. *Id.* "To extend the deliberative process privilege to a recommendation as to a particular personnel matter extends it beyond its present form to protect from disclosure what would otherwise be evidence relevant to a plaintiff's complaint of discrimination. Extension of the deliberative process privilege to such personnel matters when discrimination is charged is impossible in this Circuit." *Id*.[2]

The specific purpose behind the creation of the document will often determine whether or not the privilege is applicable. In situations where the document is created for the express purpose of addressing a particular policy, it is probable that a court would find the privilege applicable. However, if the document was created for another purpose, apart from solely addressing a particular policy, it is probable that a court would find the privilege inapplicable.

In *Tortoricic v. Goord*, 216 F.R.D, 256 (S.D. N.Y. 2003), plaintiff, the estate of a former inmate at a state psychiatric center who committed suicide, sought production of quality assurance documents generated during a review by the psychiatric center. Although defendants conceded that the documents were generated pursuant to state statute which requires a formal review upon an inmate's suicide, they refused production of the documents pursuant to the deliberative process and self-critical analysis privi-

2. Since the court had not seen the documents, an *in camera* review was ordered at which time a final decision regarding the privilege would be made. *Id.* at 163.

lege. *Id.* at 257-58. The court found that although the documents may have been considered in making the determination as to propriety of a new policy, forcibly medicating inmates at risk of suicide, they were not created for that express purpose. *Id.* Rather, the documents were created in order to measure the psychiatric center's compliance with existing procedures in light of the inmate's suicide. *Id.* Thus, the court concluded that while portions of the documents may be "deliberative," they were not prepared " 'in order to assist an agency decision maker in arriving at his decision,' " and were not "predecisional." *Id.* Accordingly, the deliberative process privilege did not apply.

Although far more common when documents are at issue, the deliberative process privilege is equally applicable to testimony. However, in light of its qualified nature, the deliberative process privilege may be overcome, not just by the government misconduct privilege as discussed above, but by a host of factors. A number of these factors require the court to engage in a classic balancing test.

In *North Pacifica v. City of Pacifica*, 274 F.Supp.2d 1118 (N.D. CA 2003), plaintiff, a developer, filed suit against defendant claiming that a certain condition imposed on approval of its project violated its equal protection rights. Dispute arose, however, as to the scope of the Pacifica City Council's members deposition testimony sought by plaintiff. *Id*. at 1120. Plaintiff's position was that it should be allowed to ask the City Council members about the decision-making process resulting in the approval of the condition and, in particular, the motive and intent of the members in approving the condition. *Id.* Defendant's position was that the testimony of the City Council members was protected by the deliberative process and attorney-client privileges. *Id*.

After reviewing the two threshold elements of the privilege, predecisional and deliberative, the court considered the following eight factors in deciding whether the deliberative process privilege should be overcome: (1) the relevance of the evidence; (2) the availability of other evidence, (3) the government's role in the litigation, and (4) the extent to which disclosure would hinder frank and independent discussion regarding contemplated policies and decisions, (5) the interest of the litigant, and ultimately society, in accurate judicial fact finding, (6) the seriousness of the litigation and the issues involved, (7) the presence of issues concerning alleged governmental misconduct, and (8) the federal interest in the enforcement of federal law. *Id.* at 1122 (internal citations omitted).

The court first considered the federal interest in the enforcement of federal law and the seriousness of the litigation and the issues involved. *Id.* at 1123. The court recognized that the federal interest in the enforcement of federal constitutional rights, in this case equal protection rights, weighed in favor of disclosure despite the fact that the litigation and the issues involved were not quite as serious as cases involving other forms of discrimination. Id at 1123-24. The court next considered the interests of plaintiff and society in accurate judicial fact finding and the relevancy of the evidence. Id at 1124.The court found that the interest in accurate judicial fact finding was heightened because equal protection rights were at stake. *Id.* Moreover, the testimony sought by Plaintiff was highly relevant because the City Council's motive and intent were central to Plaintiff's equal protection claim. *Id.* With respect to the government's role in the litigation, the court found that the decision-making process of the City Council was essentially the entire case in light of the nature of plaintiff's claim. *Id.*

The court then turned to what it considered the most important factor, the availability of other evidence. *Id.* The court rebuffed defendant's principal argument regarding this factor, namely that the information sought by plaintiff could be found in the administrative record. *Id.* at 1126.

> "...[T]he administrative record before the City Council does not exhaust the universe of information considered by the body. It is entirely possible that Council members had private conversations with the City's staff,

> NP's representatives, members of the public, and amongst themselves that are not embodied in the record. Yet this information may well be relevant in the ascertainment of motive, which is central to this case." *Id.*

Finally, the court rejected any possibility that disclosure would hinder frank and independent discussion regarding contemplated policies and decisions because it found that communications in the future were not likely to be chilled by the council members' deposition testimony. *Id.*[3] Accordingly, the court concluded that the deliberative process privilege was likely to be overcome. *Id.* at 1125.

The scope of the privilege and whether it applies to all government communications that are predecisional and deliberative or only those policy related communications that are predecisional and deliberative was at issue in a case before the Texas Supreme Court.

In *City of Garland v. Dallas Morning News*, 22 S.W.3d 351 (2000), plaintiff brought a declaratory judgment action against defendant seeking a declaration that a memorandum, from the city manager and circulated to the city council in order to discuss whether to terminate the city finance director, was not public information subject to disclosure under the Texas Public Information Act ("Act").

After determining that the memorandum was public information as contemplated under the Act, the court turned to the question of whether the memorandum was exempt from disclosure pursuant to the Act's agency memoranda exception. *Id.* at 359. The court observed that since the Act was modeled after the FOIA, the Act's agency memoranda exception, like FOIA's Exemption 5, incorporates the deliberative process privilege. *Id.* at 360. Having determined that the privilege may apply to the memorandum, the court next considered whether the privilege is limited to communications that reflect policymaking. *Id.*

Plaintiff argued that the only two conditions to applying the privilege are communications that are predecisional and deliberative. *Id.* at 361. However, the court relying on *Sears, Roebuck & Co., 421 U.S. at 151, 95 S.Ct. at 1517*, as well as a host of other federal and Texas authorities, held that the privilege is limited to policy making communications that are predecisional and deliberative. *Id.* at 364. "[I]nterpreting the deliberative process privilege to exempt any information as long as it is predecisional and deliberative would exempt all agency information except postdecisional or purely factual information. Such an interpretation would allow the exception to swallow the Act. Thus, we cannot interpret the exception so broadly." *Id.* at 364. Accordingly, the court held that the privilege did not apply to the memorandum because the memorandum did not bear on policymaking but rather simply gave the reasons to terminate the city finance director. *Id.*

An additional limitation on a defendant's assertion of the deliberative process privilege occurs when the plaintiff makes a clear showing of illegal action, misconduct, bias or bad faith on the part of the decision maker. Officials of an administrative agency cannot be compelled to testify concerning the procedure or manner in which they made their findings and rendered a decision, unless there is an allegation "and there is a clear showing of illegal or unlawful action, misconduct, bias, or bad faith on the part of the decision maker." *Gilpin County Bd. of Equalization v. Russell*, 941 P.2d 257, 264 (Colo. 1997) , citing Public *Utilities Com'n v. District Court*, 163 Colo. 462, 469, 431 P.2d 773, 777 (1967), and *Tepley v. Public Employees Retirement Ass'n*, 955 P.2d 573 (Colo. App. 1977).

The deliberative process privilege does not act as a presumption that may be rebutted merely by an allegation of misconduct; a plaintiff asserting inapplicability of the privilege must possess and provide evidence of the alleged misconduct. *Russell, supra*, 941 P.2d at 265 (holding BOE member could not, under mental process rule, be called in proceeding before BAA to explain BOE decision or how decision was reached); *Public Utilities Com'n*, 163 Colo.

3. The court imposed some limitations on plaintiff's questioning of the City Council members such as not allowing plaintiff to inquire as to the members' subjective uncommunicated thoughts. *Id.* at 1125.

at 469, 431 P.2d at 777 (1967) (mere allegation that the commissioners did not consider the entire record insufficient to compel them to testify concerning procedure or manner in which they made their findings and rendered decision in given case); *Tepley*, 955 P.2d at 578 (Colo. App. 1977) (board cannot be compelled to testify as to how and why they had reached their decision).

Other jurisdictions that have addressed the issue of probing the mental process of an administrative official through discovery requests have determined that there must be evidence of illegality before the court will even consider such requests. See *Keyes v. Lenoir Rhyne College*, 552 F.2d 579 (4th Cir.), *pet. for cert. den.*, 434 U.S. 904, 98 S.Ct. 300 (1977) (noting by implication that, in action by college faculty member for alleged employment discrimination, where allegations of discrimination are not supported by prima facie evidence, college not required to produce confidential evaluations of each faculty member on grounds that confidentiality of such evaluation records was necessary to enable college to receive honest and candid appraisals of abilities of faculty members by their peers); *Ryan v. Town of Camden*, 582 A.2d 973, 975 (Me. 1990) (affirming superior court's denial of plaintiff's discovery request to depose Board members in an attempt to establish their bias and predisposition against him).

In *Frye v. Inhabitants of Town of Cumberland*, 464 A.2d 195, 198 (Me. 1983), a police officer challenging his termination alleged, on appeal from the superior court, that the Town Manager acting as the officer hearing his appeal was biased against him. Plaintiff contended that "the superior court's failure to permit either a deposition of the Town Manager or an evidentiary hearing on the Town Manager's possible bias, improperly prevented any discovery or presentation of evidence tending to show prejudice ."[4] *Id.* at 199. The Supreme Court of Maine concluded that, although canceling the depositions altogether was improvident, a narrow protective order permitting the deposition while precisely delineating certain limited areas in which inquiry would be proscribed, was appropriate. *Id.* In making its determination, the Supreme Court acknowledged that "the general rule prohibits such inquiry [into the mental processes of an administrative decision maker] in the absence of a prima facie showing of misconduct."[5] *Id.* at 200. (*citing Citizens To Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 420, 91 S.Ct. 814, 28 L.Ed.2d 136 (1971)).

In *Carl L. Cutler Co., Inc. v. State Purchasing Agent*, 472 A.2d 913 (Me. 1984), the court elaborated on the general rule forbidding inquiry into the mental processes of an administrative decision maker. *Id.* at 918. The court stated:

> This general rule may be abrogated only when a showing of bad faith or improper behavior is strong enough to justify intrusion into the administrator's province. The requirement that the complainant adduce at least a prima facie evidence of such impro priety serves to protect the administrator from "fishing expeditions" undertaken by an disappointed bidder.

Id. The Maine Supreme Court affirmed the lower court's decision finding that the plaintiff's bare allegations that the State Purchasing Agent and vendor awarded the contract were "social friends" was not a sufficient showing to entitle plaintiff to conduct discovery of the administrator. *Id.*

FOIA Exemption 5 and the Deliberative Process Privilege

The federal Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, states in pertinent part:

4. The bias alleged by Plaintiff, in ***Frye***, consisted of his allegation that the Town Manager's involvement in the investigation of the officer's alleged violations of department regulations.

5. As a side note, the court further stated that "Frye's suggestion that a temporary lapse in procedural regularity alone should serve as grounds for this or any court to grant him reinstatement or immunity from any further proceedings with respect to these particular charges is patently erroneous." *Id.* at 198. (*citing* ***Barber v. Inhabitants of the Town of Fairfield***, 460 A.2d 1001 (Me. 1983).

> (b) This section does not apply to matters that are -
>
> ****(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.

In order for a document to qualify under Exemption 5, two conditions must be satisfied. First, the source of the document must be a Government agency. *Dep't of the Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8, 121 S.Ct. 1060, 1065, 49 L.Ed.2d 87 (2001). Second, the document must fall within the bounds of a civil discovery privilege. *Id.* One of the privileges contemplated by the second condition is the deliberative process privilege. *Id.* In order to come within the deliberative process privilege of Exemption 5, a government document must be both "predecisional" and "deliberative." *Parke, Davis & Co. v. Califano*, 623 F.2d 1, 6 (6th Cir. 1980). A document is predecisional when it is "received by the decision maker on the subject of the decision prior to the time the decision is made," *N.L.R.B. v. Sears, Roebuck & Co.*, 421 U.S. 132, 151, 95 S.Ct. 1504, 1517 (1975); and deliberative when it "reflects the give-and-take of the consultative process." *Coastal States Gas Corp. v. Department of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980).

Over the years, the first condition of Exemption 5 has been interpreted broadly by some Courts of Appeals to include communications between Government agencies and outside consultants. See *Government Land Bank v. GSA*, 671 F.2d 663 (1st Cir 1982); *Hoover v. U.S. Dept. of Interior*, 611 F.2d 1132 (5th Cir. 1980); *Lead Industries Assn. v. OSHA*, 610 F.2d 70 (2nd Cir. 1979). The Supreme Court, however, recently narrowed the first condition in a case where the government attempted to stretch the definition of "outside consultant."

In *Dep't of the Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 121 S.Ct. 1060, 149 L.Ed.2d 87 (2001), the issue before the Court was whether documents, exchanged between Indian Tribes and the United States Department of the Interior addressing tribal interests subject to state and federal proceedings, were exempt from the disclosure requirements of FOIA because of their status as "intra-agency memorandums or letters."

The case arose out of the Department of Interior's Bureau of Indian Affairs ("the Bureau") filing claims on behalf of the Klamath Tribe and other tribes in a state court suit intended to allocate water rights. Prior to filing suit, the Bureau consulted with and exchanged written memoranda with the tribes regarding potential claims. *Id.* at 5. The Klamath Water Users Protective Association, whose interest were adverse to the interests of the tribes, filed a series of requests with the Bureau under the FOIA seeking access to the memoranda and other communications exchanged between the Bureau and the tribes. *Id.* at 6. Despite producing some documents, the Bureau withheld others as exempt under the attorney work-product and deliberative process privileges pursuant to Exemption 5 of the FOIA. *Id.* at 6.

On certiorari review of the Ninth Circuit's opinion that Exemption 5 did not apply to bar disclosure of the documents, 189 F.3d 1034 (1999), the Supreme Court found the Department's apparent position, that the inter-agency or intra-agency communications condition should be placed on any document the Government would find valuable to keep confidential, untenable. *Id.* at 12. "There is, however, no textual justification for draining the first condition of independent vitality, and once the intra-agency condition is applied, it rules out any application of Exemption 5 to tribal communications on analogy to consultants' reports." *Id.*

The Court was not persuaded by the Department's argument that the tribes were akin to outside consultants whose records played essentially the same part in the Department's deliberation as those documents prepared by the Department itself. *Id.* at 10. The Court observed that those consultants whose communications have typically been held exempt had not been com-

municating with the Government in their own interest or on behalf of any person or group whose interest might be affected by the Government action addressed by the consultant. *Id.* The tribes, however, communicated with the Bureau with their own interest in mind. *Id.* "While this fact alone distinguishes tribal communication by several Courts of Appeals, the distinction is even sharper, in the Tribes are self-advocates at the expense of others seeking benefits inadequate to satisfy everyone." *Id.* The Court concluded that there was simply no support for the "Indian trust" exemption sought by the Department given the FOIA's mandate of broad disclosure. *Id.* at 16-17.

In a recent case from the Second Circuit, the Government, armed with far better facts, successfully utilized the same argument for the non disclosure of documents that the Supreme Court rejected in *Klamath*.

In *Tigue v. Dep't of Justice*, 312 F.3d 70 (2nd Cir. 2002) the court found that a memorandum prepared by an Assistant U.S. Attorney in the Southern District of New York and forwarded to the Criminal Investigation Division Review Task Force, established by the IRS and known as "the Webster Commission," was shielded by FOIA's Exemption 5 as reflecting an agency's deliberative process. The memorandum at issue outlined the Southern District's opinions and recommendations with respect to how the IRS should conduct criminal tax investigations. *Id.* at 73. Plaintiff, while conceding that the memorandum was at least in part deliberative, argued that the memorandum was not protected by the deliberative process privilege because it was neither an inter-agency or intra-agency document nor a predecisional document. *Id.* at 76.

Turning first to the inter-agency or intra-agency issue, the court initially noted that the Supreme Court in *Klamath* cautioned that the term "intra-agency" is not " ' just a label to be placed on any document the Government would find it valuable to keep confidential.' " *Id.* at 77 quoting *Klamath*, 532 U.S. at 12. " ' [W]hether a particular document is exempt under (b)(5) depends not only on the intrinsic character of the document itself, but also on the role it played in the administrative process.' " *Id.* at 78 quoting *Lead Industries Assn. v. OSHA*, 610 F.2d 70 (2nd Cir. 1979). Unlike the tribes in *Klamath*, who clearly had their own interests in mind in communicating with the Bureau of Indian Affairs, the court observed that the Webster Commission was not acting on its own behalf in requesting the memorandum at issue. *Id.* Rather, the Webster Commission was acting as a consultant to the IRS in order to assist the IRS with developing policy recommendations. *Id.* at 78. As such, the court found that the memorandum generated by the Southern District was an inter-agency communication because it was intended to assist the Webster Commission with its responsibilities to the IRS. *Id.* at 79. "To conclude that the deliberative process privilege does not apply when an outside consultant to an agency receives information from another agency effectively would condition the use of consultants on both agencies' willingness to disclose any information the consultant reviews in the process of its work and would unreasonably hamper agencies in their decision-making process." *Id.*

With respect to the predecisional issue, the court found that the memorandum was not simply a part of a routine and ongoing process of agency self-evaluation as was the case in *Maricopa Audubon Society v. United States Forest Service*, 108 F.3d 1089 (9th Cir. 1997)(holding that the government must show that the predecisional material was prepared to assist the agency in the formulation of a specific decision). *Id.* at 80. Rather, the memorandum was specifically prepared for use by the Webster Commission in advising the IRS on its future policy with respect to the Criminal Investigation Division. *Id.* Accordingly, the court found that the memorandum was predecisional despite the fact that the IRS may not have made a specific decision in reliance on the memorandum. *Id.*

Given the rulings in *Klamath* and *Tigue*, proper application of FOIA's Exemption 5 as it relates to the deliberative process priv-

ilege and the Government's ever increasing reliance on outside consultants should now be easier to define. Appellate and trial courts, however, will likely view the Government's characterization of an entity as an outside consultant with a more jaundiced eye. As such, the Government will be forced to spend substantially more time convincing the court that its communications with outside consultants constitute inter-agency or intra-agency materials.

State courts often look to the law of the Federal Freedom of Information Act in interpreting the deliberative process privilege as it applies to Open Records Act requests. See, e.g., *Colorado Springs v. White*, 967 P.2d at 1049.

In two cases interpreting the exemptions under FOIA, predecisional deliberative documents were withheld from plaintiffs. In *American Federation of Gov't Employees, Local 2782 v. U.S. Dep't of Commerce*, 907 F.2d 203 (D.C. Cir. 1990). Unsuccessful promotional applicants sought production of copies of forms and promotion-related memoranda reflecting or potentially reflecting opinions and discussions regarding job performance of the plaintiffs and other candidates for promotion. *AFSCME v. Dep't of Commerce*, 907 F.2d at 206-208. The District of Columbia Circuit held that the requested material was subject to the deliberative process privilege, and thus not available to the plaintiffs. *Id.* Similarly, the U.S. 11th Circuit Court of Appeals determined that an attorney who served as a Deputy Regional Attorney but was the unsuccessful candidate for the position of Regional Attorney was not entitled to the entire contents of his promotional file under the Freedom of Information Act. *Stephens v. Dep't of Health & Human Services*, 901 F.2d 1571, 1577 (11th Cir. 1990).

In a similar vein, in *Schell v. United States Dep't of Health & Human Services*, 843 F.2d 933 (6th Cir. 1988), the United States Court of Appeals for the Sixth Circuit determined that the plaintiff, an attorney-advisor in a field office of the Official of Hearings and Appeals for the Social Security Administration could not obtain a memorandum prepared by Administrative Law Judges for the Social Security Administration responsive to criticism of their operations because it was protected by Exemption 5. *Schell*, 843 F.2d at 940. The 6th Circuit further determined that the memorandum was protected as part of the deliberative process whether or not it was solicited, and whether or not it actually was considered in making decisions. *Schell*, 843 F.2d at 941. The 6th Circuit reasoned that allowing disclosure in any circumstances would run afoul of the very reason for application of the deliberative process, that is, to encourage frank and open communication among public officials and employees. *Id.*

Cases in Which the Deliberative Process Privilege May Play a Role

The recent events involving Vice President Richard Cheney and the group known as "The Energy Task Force" provide the opportunity for consideration of the applicability of the deliberative process privilege to the highest reaches of the federal government. The United States Supreme Court granted certiorari on the propriety of discovery concerning the Vice President's task force. *See Cheney, Vice President of U.S. v. USDC DC*, ___ S.Ct. ___ (Mem), 2003 WL 22251301 (U.S.), 72 USLW 3248.

In the underlying case, *Judicial Watch, Inc. v. National Energy Policy Development Group*, 219 F.Supp.2d 20 (D.D.C, 2002), plaintiffs filed suit against Vice President Cheney, the National Energy Policy Development Group ("NEPDG"), various federal officials and private individuals to enforce certain requirements of the Federal Advisory Committee Act ("FACA"), the Freedom of Information Act ("FOIA"), the Administrative Procedures Act ("APA") and the federal mandamus statute. Specifically, plaintiffs sought information concerning the activities of the NEPDG and its members in developing and recommending a national energy policy to President Bush. *Id.* at 24. Defendants moved to dis-

miss raising a number of jurisdictional, statutory and constitutional objections.

One of the more interesting objections raised by the defendants related to the separation of powers. "The constitutional question suggested by this case is whether Congress can pass a law granting the public access to the deliberative process of a formally constituted group of the President's advisors when at least one of those advisors is a private individual without violating Article II." *Id.* at 44. Due to the complete absence of any discovery, the court declined to substantively address this issue until further factual development. *Id.* at 46. Nevertheless, the court observed that once the constitutional issue is properly before it, it will have to carefully balance whether FACA's requirements would infringe the President's ability to perform his constitutional functions and whether that impairment is outweighed by any constitutionally authorized Congressional purposes. *Id.* at 50.

The deliberative process privilege may end up playing a significant role in the court's determination of the constitutional issue. As the court observed, FACA, pursuant to the FOIA exemptions, has two important exceptions to the requirement that the public have access to meetings and documents. *Id.* at 53-54. Those exceptions are deliberative process and national security concerns. *Id.* Again, however, the court chose not to address those questions until further factual development had taken place including a determination of who participated in the deliberations of the NEPDG, the nature of the interactions with the president, the role of the Vice President in the deliberations and the proximity of these individuals and the NEPDG to the President. *Id.* at 44, 53.

Conclusion

The deliberative process privilege is a protective shield for lawyers defending governmental agencies and officials. Its protection, however, is not without limits. Lawyers who deal with governmental agencies or who litigate against those agencies must prepare themselves with counter measures to pierce the privilege.

The Privacy Project II

The Self Critical Analysis Privilege in Medical Care: The Law is One Thing in Rome and Another in Athens

By Paul E. Svensson and George S. Hodges

Paul Edward Svensson, an associate at Boeggeman, George, Hodges & Corde, P.C. of White Plains, NY, and graduated from Pace Law School. He attended Holy Cross College and has a M.P.H. in Health Administration from the University of Pittsburgh. Prior to practicing law, he was a hospital administrator. He is licensed to practice law in New York, Connecticut and New Jersey.

George S. Hodges is managing partner of Boeggeman, George, Hodges & Corde, P.C. He is a graduate of Fordham University School of Law, having received his J.D. degree in 1973. Mr. Hodges is the President-Elect of the IADC. He is also the chair of the Privacy Project editorial board.

Introduction

Health information is among the most personal and sensitive of any maintained about an individual. As the nation's medical care system continues to develop and share its informational database with a wide variety of providers, insurance payers and regulatory agencies, the susceptibility of that information to disclosure also increases. The federal government has taken preliminary steps to protect this information with the enactment of the Health Care Quality Improvement Act (HCQIA),[1] and the Health Insurance Portability and Accountability Act (HIPAA)[2] and its component Federal Privacy Rule.[3] However, neither HCQIA nor HIPAA provide sufficient statutory protection of data used for medical peer review, or self-critical analysis, purposes. The gap has been partially filled by a diverse mix of state statutory privileges.

The Significance of Privileged Analysis

At tension in the law of privileges is, on the one hand, the public benefit that comes from keeping certain information confidential and, on the other hand, the public benefit that comes from ascertaining the truth of the matter, as facilitated by the discovery of all relevant information. Thus, to recognize self-critical analysis as privileged, its protection must promote an important interest that outweighs the need for probative evidence.[4]

Medical peer review is a function performed by members of the medical and nursing staffs to address quality care issues. Such reviews may include identifying correctable trends in the standard of medical care delivered by individual physicians and nurses, evaluating adverse events, establishing clinical guidelines and evaluating applicant qualifications for the award and/or renewal of medical and nursing staff privileges. Peer review has been used since 1952, when the Joint Commission on the

1. 42 U.S.C. §§ 11101-11145 (West 2003); see also H.R. Rep. No. 99-903 (1986), reprinted in 1986 U.S.C.C.A.N. 6384 (explaining the need to improve the quality of health care by conducting peer review, identifying and reporting review actions affecting clinical privileges to a national databank in order to identify incompetent physicians and restrict their movement).

2. 42 U.S.C. 1320d-8 (West 2003).

3. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. 160, 164 (2003).

4. *See* Trammel v. United States, 445 U.S. 40 (1980)(clergy-penitent privilege); UpJohn Co. v. U.S., 449 U.S. 383 (1981)(attorney-client privilege); University of Pa. v. EEOC, 493 U.S. 182 (1990)(no academic peer review privilege); Jaffee v. Redmond, 518 U.S. 1 (1996)(psychotherapist-patient privilege).

Accreditation of Hospitals first imposed the requirement on the medical staffs of its member hospitals.[5] State regulatory agencies had mandated peer review activities and established reporting requirements before the enactment of HCQIA in 1986, but HCQIA expanded the application of reportable incidents involving medical practitioners to a national database. As such, medical peer review is one of the primary means of ensuring the continued improvement of quality patient care within the medical and nursing professions.

Purpose of this Paper

This paper discusses the availability and application of a self-critical analysis privilege in the medical peer review context. In general, and specifically for the purposes of this paper, the terms self-critical analysis and peer review are considered analogous and may be used interchangeably.

Part I will acknowledge the absence of a medical self-critical analysis privilege in the federal common law and discuss the application of the federal law of privileges under Fed. R. Evid. 501. Part II will review the historical role of the states in forming health policy, the doctrine of federal preemption, the development of federal legislation to protect limited aspects of medical peer review and patient privacy interests, and the preemptive effect of the federal legislation on state statutes. Part III will discuss the relevant federal court decisions which have addressed the application of a medical peer review privilege. Part IV will review representative state statutes providing medical peer review privileges and discuss a rationale for extending state privileges to federal court claims. Part V will conclude that the absence of a uniform self-critical analysis privilege has serious ramifications for medical care providers.

PART I

Status of Peer Review Privilege in Federal Common Law

It is well settled that there is no physician-patient privilege recognized in the federal common law.[6] Even though the U.S. Supreme Court has opined that the physician-patient privilege is "rooted in the imperative need for confidence and trust,"[7] to date, Congress has not codified this concept in a federal statute. On the contrary, this privilege has been codified by essentially all state legislatures.

Likewise, no medical peer review, or self-critical analysis, privilege is found in the federal common law.[8] While states have been aggressive in developing statutory authority, such medical peer review privileges are not conclusive in cases brought in federal court under federal law.[9]

In *Jaffee v. Redmond*, the Supreme Court set forth principles to be considered in determining when Fed. R. Evid. 501 authorizes federal courts to define new privileges under the federal common law.[10] As noted above, the privilege must promote "sufficiently important interests to outweigh the need for probative evidence."[11] Moreover, the analysis must be made on a case-by-case basis, and take into account both the private and public interests that the privilege serves, as well as the evidentiary benefit that would result if the privilege were denied.[12] Finally, the Court has explained that any privilege must be strictly construed.[13]

In accordance with this directive, the Court enumerated a four-part test for judging whether such a self-critical analysis privilege applies. First, the information must be self-critical analysis undertaken by the party seeking the protection. Second, the public must have a strong interest in maintaining the flow of the information.

5. The Joint Commission on the Accreditation of Healthcare Organizations (JCAHO), formerly JCAH, still requires its member facilities to participate in a peer review process.
6. *See* Whalen v. Roe, 429 U.S. 589, 602 n. 2 (1977).
7. 445 U.S. at 51.
8. Univ. of Pa. *supra* note 4.
9. *See* Holland v. Muscatine General Hospital, 971 F. Supp. 385, 388 (S.D. Iowa 1997); *see also* Von Bulow v. Von Bulow, 811 F.2d 136, 141 (2d Cir. 1987).
10. 518 U.S. at 8.
11. *Id.* at 9; see also Univ. of Pa. *supra* note 4.
12. *Id.* at 8.
13. 493 U.S. at 189.

Third, the information must be of a type whose flow would be curtailed if discovery were allowed. Fourth, the information must have been created with the expectation that it would be kept confidential, and it has in fact been kept confidential.[14] Although federal courts have applied a similar methodology in determining whether a self-critical analysis relative to peer review material exists, as will be discussed below, there is lack of unanimity in finding a privilege.[15]

Finally, as will be discussed more fully below, the presence and breath of a federal statutory privilege has been widely contested. To date, only one federal court has recognized and incorporated state statutory privileges in finding that the state policy was consistent with the federal policies implicated in the case.[16]

Evidentiary Considerations in Federal Court

It is well settled that when resolving an action involving a federal question, the federal common law of privileges would apply under Fed. R. Evid. 501.[17] Conversely, in a diversity case in which only state claims were raised, state law would govern.[18]

There is, however, one contrary federal court decision in which a state medical peer review privilege was applied to a federal civil rights claim.[19] Consistent with the Supreme Court dicta in *Jaffee*, the court in *Does v. St. Joseph* found that Fed. R. Evid. 501 was intended to permit the consideration of state law and policy and encourage "flexibility to develop rules of privilege on a case-by-case basis."[20] However, in a later decision, the same Indiana District Court in *Mattice v. Mem. Hosp. of South Bend* distinguished this finding and clarified that the *St. Joseph's* court had upheld the peer review privilege under the particular circumstances of that case because the plaintiff had failed to allege facts from which an inference of workplace discrimination could arise.[21] In other peer review cases, *St. Joseph's* has met with criticism based upon its interpretation of Fed. R. Evid. 501.[22] This does not, however, question the view of the Supreme Court that Fed. R. Evid. 501 is designed to be flexible.

In cases where state law claims are raised pendent to federal claims, the question of choice of law becomes more difficult.[23] Literally read, Fed. R. Evid. 501 would appear to require the Court to apply the federal common law of privileges with respect to the federal claims and the state law of privileges with respect to state claims. However, such dual application was not the clear intent of Congress. A review of the legislative history shows that Fed. R. Evid. 501 was developed based on the understanding:

> (1) privilege rules were and should continue to be considered substantive for *Erie* purposes;
> (2) privilege rules were outcome determinative;
> (3) where State law supplied the rule of decision, State rules of privilege should be applied because there is no Federal interest substantial enough to justify departure from State policy; and
> (4) State policy regarding privilege should not be thwarted merely because of diversity jurisdiction, a situation, which, if allowed, would encourage forum shopping.[24]

14. Dowling v. American Haw. Cruises, 971 F.2d 423, 425-26 (9th Cir. 1992).

15. *See* Holland *supra* note 8 (action alleging a hostile work environment in violation of the Civil Rights Act of 1964, 42 U.S.C.S. § 2000e et seq., and Iowa Code § 216); Pagano v. Oroville Hosp., 145 F.R.D. 683 (E.D. Cal. 1993)(court declined to recognize self-critical privilege where the peer review process itself was under attack) *and compare* Bredice v. Doctors Hosp., Inc., 50 F.R.D. 249 (D.D.C. 1970)(peer review materials privileged in medical malpractice action), Weekoty v. United States, 30 F. Supp. 2d 1343 (D.N.M. 1998)(self-critical privilege extended to morbidity and mortality analysis),

16. *See* Wei v. Bodner, 127 F.R.D. 91, 94-5 (D.N.J. 1989).

17. Fed. R. Evid. 501 states, in part, that privilege "shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in light of reason and experience."

18. Fed. R. Evid. 501 concludes: "However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law." *See also* Morse v. Gerity, 520 F. Supp. 470 (D. Conn. 1981).

19. Does v. St. Joseph's Hosp., 113 F.R.D. 677 (N.D. Ind. 1987).

20. *Id.* at 679 (citing Trammel, 445 U.S. at 47).

21. Mattice v. Memorial Hosp. of South Bend, 203 F.R.D. 381 (N.D. Ind. 2001).

22. *See e.g.*, Nilavar v. Mercy Health System - Western Ohio, 210 F.R.D. 597 (S.D. Ohio 2002).

23. *See generally*, Krolikowski v. Univ. of Massachusetts, 150 F. Supp. 2d 246 (D. Ma. 2001).

24. H.R. Rep. No. 650, 93rd Cong., 1st Sess. 9 (1973).

Thus, it is commonly held that in federal question cases, even where pendent state claims are raised, the federal common law governs all claims of privilege raised in the litigation.[25] This was the approach suggested by the Senate Judiciary Committee and is generally acknowledged to be the approach most consistent with the policy of Fed. R. Evid. 501. That policy, simply stated, is that "in non-diversity jurisdiction civil cases, federal privilege law will generally apply."[26] Nonetheless, *Jaffee* authorizes federal courts to define new privileges under the federal common law where the privilege promotes an interest that outweighs the need for probative evidence.

To date, there has only been one federal court decision where a state law peer review privilege has been applied to a pendent state law claim.[27] As will be discussed more fully below, the position of the court in *Cohn v. Wilkes Gen. Hosp.* is insupportable because the plain language of the HCQIA immunity provision relied upon by the court does not include materials produced under peer review.

The Importance of Confidentiality to the Medical Self-Critical Analysis Privilege

Confidentiality is essential to meaningful and effective medical peer review. The importance of confidentiality in the law of privilege has long been recognized. Professor John Henry Wigmore is generally credited with having articulated the requirements for recognizing common law privileges most frequently cited by courts. These include: (1) the communications must originate in a confidence that they will not be disclosed, (2) the element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties, (3) the relationship must be one which in the opinion of the community should be diligently fostered, and (4) the injury that would inure to the relationship from disclosure of the communication must be greater than the benefit to be derived for purposes of litigation.[28]

The law of privileges is not just a rule governing the admissibility of evidence. Its primary purpose is to protect the confidentiality of communications in circumstances where such confidentiality serves broad societal goals. Once confidentiality is broken, the basic purpose of the privilege is defeated. The self-critical analysis privilege is premised upon the philosophy that frank and potentially damaging self-criticism should be confidential and protected from discovery in order to encourage the performance of an activity with obvious social benefits.[29] As such, the policies behind the medical peer review privilege and liberal discovery conflict, and federal courts have struggled mightily while reaching divergent outcomes as to whether documents created and reviewed during peer review are discoverable for use in civil litigation. State legislatures have enacted laws in the absence of a single federal authority and, these statutes combined with the case law, form a crazy quilt of regulations that fails to define a uniform national policy.

PART II

The Historical Role of the States in Forming Health Policy

In a compromise between competing ideologies, the United States Constitution established a union among states with broad sovereign powers and a national government of supreme, albeit enumerated, powers. The sovereign powers retained by the states under the Constitution, collectively known as the police powers, constitute the primary source of governmental authority for the states to act to protect the public health.[30]

25. *See* S.Rep. No. 1277, 93d Cong., 2d Sess. 12 n.16 (1974), reprinted in 1974 U.S.C.C.A.N. 7059 n.16.

26. H.R. Rep. No. 1597, 93d Cong., 2d Sess. 7 (1974), reprinted in 1974 U.S.C.C.A.N. 7101.

27. Cohn v. Wilkes General Hosp., 127 F.R.D. 117 (W.D.N.C. 1989).

28. *See* 8 John Wigmore, Wigmore on Evidence 2285, at 527 (3 ed. 1940).

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

30. *See* Sporhase v. Nebraska ex. rel. Douglas, 458 U.S. 941 (1982) ("a state's power to regulate . . . for the purposes of protecting the health of its citizens . . . is at the core of its police power"). *See also*, e.g., Medtronics, Inc. v. Lohr, 518 U.S. 470, 474-75 (1996)("the State's traditionally have had great latitude under their police powers to legislate as to the protection of the . . . health . . . of all persons").

In *Jacobsen v. Massachusetts*,[31] the Supreme Court asserted the primacy of state authority in enacting public health laws,[32] in holding that such regulations are permissible when they were: (1) "necessary of the case," (2) not exercised in "an arbitrary, unreasonable manner," (3) "reasonably required for the safety of the public," and (4) "tend[ed] to promote the general welfare."[33] This deferential standard of review requires that the governmental purpose be valid, the means reasonable, and the means reasonably directed towards achieving the objective. The Supreme Court has established more exacting standards where certain individual rights are affected by public health measures, including the application of procedural and substantive due process under the Fifth[34] and Fourteenth[35] Amendments, and equal protection of the law under the Fourteenth[36] Amendment in determining whether to uphold public health regulations that affect personal liberties.[37]

The federal government essentially left exclusive control of matters affecting the public health to the states until the early twentieth century when several factors led to a shift in political philosophy. The more notable factors included the change in the economic nature of the country from an agrarian to an industrial society resulting in great population increases in urban areas and an increased reliance on interstate commerce. In healthcare, the determinative reason for federal involvement has been the growth of federal government expenditures as an insurer of medical care services.

The Federal Preemption Doctrine

Federal preemption of state law relates to the proper distribution of federal and state power. Federal laws generally include express preemption language as well as savings provisions, limiting the breath of express statutory preemption. In the absence of an express congressional intent to preempt state law, federal law can still serve as a barrier to the application of state law under the theory of implied preemption.[38]

Implied preemption arises in two contexts. In both cases, the crucial inquiry is whether Congress, in establishing the particular statute, intended to exercise its constitutionally delegated authority to set aside the laws of the states. In the first instance, implied preemption will be found if a federal enactment occupies a field so completely "as to make reasonable the inference that Congress left no room for the states to supplement it."[39] The Court has held that when the field is one traditionally occupied by a state, the historic police powers of the state should not be lightly superseded,[40] unless Congress expresses a clear and manifest intent to occupy the entire field of regulation.[41] Alternatively, implied preemption may arise when state law actually conflicts with federal law. This occurs where: (1) "compliance with both federal and state regulations is a physical impossibility,"[42] or (2) when state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[43]

Thus, any incompatibility between state and federal law required the courts to con-

31. 197 U.S. 11 (1905)

32. *Id.* at 34.

33. *Id*. at 28.

34. U.S. Const. amend. XIV ("No state shall . . . deprive any person of life, liberty, or property, without due process of law. . .").

35. U.S. Const. amend. XIV ("No state shall . . . deny to any person within its jurisdiction the equal protection of the laws."); *see also* Bolling v. Sharpe, 347 U.S. 497 (1954) (holding that equal protection applies to the federal government through the Due Process Clause of the Fifth Amendment).

36. U.S. Const. amend. XIV ("No state shall . . . deny to any person within its jurisdiction the equal protection of the laws."); *see also* Bolling v. Sharpe, 347 U.S. 497 (1954) (holding that equal protection applies to the federal government through the Due Process Clause of the Fifth Amendment).

37. Washington v. Glucksberg, 521 U.S. 702, 713 (1997)(requiring "a careful description" of the individual liberty interest, and that the interest be "deeply rooted in the Nation's history and tradition.").

38. *See* Shaw v. Delta Airlines, Inc., 463 U.S. 85 (1983).

39. Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947).

40. *See* Jones, 430 U.S. at 525.

41. *See* Philadelphia v. New Jersey, 437 U.S. 617, 621 n.4 (1978).

42. Florida Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142-43 (1963).

43. Hines v. Davidowitz, 312 U.S. 52, 67 (1941).

duct a plain language reading of the federal statute, and determine whether Congress intended the federal law to have precedent effect.[44] Federal courts have generally acted judiciously in applying the preemption doctrine so as not to risk ousting state power in areas where the state has a substantial interest in regulating the conduct at issue.[45]

Federal Health Legislation

As noted above, two federal laws implicate the medical self-critical analysis privilege, but neither HCQIA nor HIPAA adequately address the need for a medical peer review privilege.

The Health Care Quality Improvement Act

The purpose of HCQIA was to identify incompetent physicians and to report them to a national data bank where this information could be disseminated to other providers. The primary method for identification of these physicians was, and continues to be, the medical peer review process. As an incentive to encourage peer review activities, HCQIA provides a qualified immunity for participants in the peer review process relative to federal and state civil actions arising from these activities on or after October 14, 1989.[46] Immunity, however, is not available where peer review participants fail to provide the minimum procedural safeguards outlined by HCQIA.[47] More importantly, only one federal court has found that this immunity extends to materials arising from the medical peer review process under 42 U.S.C. § 11111.[48]

Importantly, HCQIA does protect, as confidential information, reports of adverse actions taken against physicians made to the national practitioners data bank, with the exception that confidentiality does not extend to unidentifiable health information regarding physicians, health care entities or patients.[49] As will be developed more fully below, federal courts have split in their decisions whether the federal peer review privilege under 42 U.S.C. § 11137 extends to all materials arising from the medical peer review process.

As regards the preemptive status of HCQIA relative to state laws, in 1987 Congress amended 42 U.S.C. § 11115 by adding language stating that nothing in the statute "shall be construed as changing the liabilities or immunities under law or as preempting or overriding any state law" that affords members of the review process greater "immunities or protection" than those found within the statute.[50] Thus, HCQIA does not limit either the defenses or immunities available to physicians, nor does the statute affect the rights and remedies afforded patients to seek redress for medical malpractice,[51] under any provision of federal or state law.

The addition of this savings language, protecting state immunity provisions, is significant. By acknowledging the existence of greater state law immunities and protections and not providing a federal privilege to limit the discovery of peer review documents, it is arguable that Congress demonstrated an intent not to establish a federal privilege. However, it is equally arguable

44. 505 U.S. 504, 523 (1992)(the Supreme Court indicated that it need "not look beyond" the plain language of the preemption provision to examine congressional intent where the provision was unambiguous); *see also* 518 U.S. 470, 484 (1996)(the Supreme Court, in finding that the statutory language was ambiguous, insisted that the congressional intent underlying the statute be considered to determine whether it supported the preemption of state law).

45. *See* Farmer v. United Bhd. Of Carpenters, 430 U.S. 290, 302 (1977).

46. *See* 42 U.S.C. § 11151(11)(defined as a "health care entity and the governing body or any committee of a health care entity which conducts professional peer review activity, and includes any committee of the medical staff of such entity when assisting the governing body in a professional review activity.")

47. *See* 42 U.S.C. § 11112(b)(listing guidelines relative to hospitals for review to trigger immunity and standard of review for immunity to attach). These procedural safeguards include that the professional review action is taken to further enhance quality health care, necessary facts are obtained and the subject of the review has had adequate notice and a hearing and there is reasonable belief that the facts warranted the action.). On the contrary, physician groups and HMOs are covered only if they have a formal peer review process that meets established criteria. *See* 42 U.S.C. § 11151(4)(a)(i)(ii); C.F.R. 60.2 (2003).

48. Cohn *supra* note 26.

49. *See* 42 U.S.C. § 11137(b)(1).

50. Pub. L. No.: 100-177, § 402(c) codified at 42 U.S.C. § 11115(a).

51. *See* 42 U.S.C. § 11115(d).

that Congress recognized that since states had developed laws regarding confidentiality of peer review materials there was no reason to alter the effect of these laws.

The problem for the defendant attempting to assert a state privilege occurs, however, when pendant state claims are resolved in federal court and a limited federal privilege is applied under a strict interpretation of Fed. R. Evid. 501.

The Health Insurance Portability and Accountability Act

The purpose of HIPAA, and its Federal Privacy Rule, is to grant patients greater access to their medical records and more control over how their individually identifiable health information[52] is used.

HIPAA utilizes a similar issue preemption scheme with respect to state laws as HCQIA. State laws that are contrary and less protective than the federal regulations are preempted.[53] Whereas, state laws that are (1) contrary but "more stringent" than the federal regulations, or (2) deemed necessary to assist with state supervision over health care delivery or otherwise serve a compelling need relating to public health, safety or welfare are not preempted.[54]

Thus, HIPAA, and the federal Privacy Rule enacted under its authority, establish a floor for protecting the privacy of health information, granting states the flexibility to establish comparable or greater privacy protections. Unfortunately, HIPAA neither requires state action nor demands the development of uniform protections when states choose to act.

HIPAA also has several limitations permitting the unprotected use of both identifiable and de-identifiable health information which may indirectly have a chilling effect on medical peer review activities.

First, HIPAA does not guarantee a complete right to privacy. This is particularly interesting in light of federal court rulings based upon constitutional claims of privacy. In *Whalen v. Roe*, the Supreme Court squarely faced the question whether the constitutional right to privacy encompasses the collection, storage and dissemination of health information in government data banks. The Court failed to provide a meaningful constitutional remedy but did acknowledge that a duty to avoid unwarranted disclosure was rooted in the federal Constitution.[55] Federal courts have generally interpreted the dicta of the Supreme Court as affording a tightly circumscribed right to informational privacy or have grounded the right to privacy in state constitutions.[56]

Second, a restrictive delegation of authority leaves several entities which collect health information unprotected. HIPAA covers only certain entities engaging in the electronic transmission of data, including health plans, health care clearinghouses and health care providers.[57] Thus, health care providers who really solely on paper claims, employers, life insurers, and entities who receive health information from covered health care providers, such as third-party administrators, researchers, public health officials and contractors, are excluded.[58]

Under HIPAA, covered entities are required to disclose identifiable health information in two circumstances, but may use or disclose identifiable health information whenever authorized by the individual patient, or otherwise permitted under the Privacy Rules.[59]

Disclosure is mandated where an individual patient requests his or her own protected information, and when the Secretary of Health and Human Services is investigating a complaint or determining a covered entity compliance with the HIPAA Privacy

52. 45 C.F.R. 164.501 (2003).

53. 45 C.F.R. 160.203 (2003)(detailing the process of preemption).

54. 45 C.F.R. 160.203(b); 45 C.F.R. 202 (2003).

55. 429 U.S. at 605; *see also* Nixon v. Administrator of General Services, 433 U.S. 425 (1977)(hesitantly acknowledging a narrow right to privacy);

56. *But see* J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981)(holding that the right to privacy does not extend to a general right to nondisclosure of personal information)

57. 45 C.F.R. 160.102 (2003); *see* 42 U.S.C. 1320D-2 (2003).

58. 64 Fed. Reg. 59924 (Nov. 3, 1999)

59. 45 C.F.R. 164.502(2003).

Rules. Generally, a covered entity is permitted to use or disclose identifiable health information for the purpose of its health care operations (including business purposes and medical peer review activities) or when the information has been de-identified.

Identifiable information may also be used or disclosed for judicial and administrative proceedings, under protective order, so long as the individual has an opportunity to object and those objections have been resolved.[60]

In medical peer review activities, identifiable patient information is used, under HIPAA authority, but is routinely de-identified as part of the analysis of the care delivered by the health care provider. HIPAA fails to protect de-identified data. Health care providers are therefore left to seek protection under HCQIA and state statutory protections. As noted above, HCQIA extends certain protection where information, used for peer review purposes, has been de-identified as to patients but practitioners and/or health care entities remain identifiable. The question is: what protection does HCQIA actually offer?

PART III

Representative Federal Court Decisions

As discussed above, federal courts have split in their decisions whether either HCQIA peer review privilege, referenced in 42 U.S.C. § 11111(a)(1) and 42 U.S.C. § 11137(b)(1), extends to all materials arising from the medical peer review process.

With the exception of the decision in *Cohn*, no federal court has found that the limited immunity provided by 42 U.S.C. § 11111(a)(1) extends a privilege to materials developed or reported as a result of peer review activities. The *Cohn* court relied more heavily on the mere existence of HCQIA rather than focusing on the actual statutory language and, as such, is a questionable decision. On its face, 42 U.S.C. § 11111(a)(1) only grants a limitation on damages for those who participated in the peer review process, unless the entity or person seeking protection violated the civil rights of the person subject to review and seeking disclosure of the materials.[61] As such, the relevant sections of HCQIA relied upon by the *Cohn* court fail to create a federal privilege for documents prepared in the course of peer review activities.

On the other hand, there is a difference of opinion between federal courts whether 42 U.S.C. § 11137(b)(1) extends to all documents arising from the medical peer review process. Section 11137(b)(1) provides a privilege for the information which entities are required to "report" to the national data bank.[62] As will be seen, courts which have denied the availability of a privilege emphasize that the plain language does not extend to information "gathered" during the peer review process. However, as noted above, decisions as to the preemptive effect of federal statutes extend beyond a mere plain language reading of the statute. Courts are also charged with the duty to ascertain the intent of Congress in enacting the legislation and to consider whether this is an area where they should apply a flexible interpretation of Fed. R. Evid. 501 as the Supreme Court encouraged in *Jaffee*.

Decisions regarding this statute have been reached in cases as diverse as employment discrimination, civil rights, antitrust, Federal Tort Claim Act and medical malpractice actions.

Courts that have denied a peer review privilege have considered the applicability of state privilege laws[63] but, as noted above, the *St. Joseph's* case remains the only application of state laws to this federal question. Most courts emphasize that the HCQIA privilege provided under 42 U.S.C. § 11137(b)(1) is limited to information "reported" to the national data bank.[64] Thus,

60. *See e.g.*, Ex. Rel. Mary Jane Stewart v. The Louisiana Clinic, 2002 U.S. DIST. LEXIS 24062 (E.D.La. Dec. 12, 2002)(In this False Claims Act case, the court allowed the government to use protected patient information for this litigation and its health oversight activities after resolution of objections to redact and for protective order.)

61. 42 U.S.C. § 11111(a)(2); *see also* Patrick v. Burget, 486 U.S. 94 (1988) *and* Summit Health, Ltd. v. Pinhas, 500 U.S. 322 (1991).

62. 42 U.S.C. § 1131-1133 (2003).

63. *See e.g.*, 791 F. Supp. 188.

64. *See e.g.*, 198 F.R.D. 1.

the omission by Congress to expressly provide a privilege for all materials produced in peer review has been cited as a rationale for denying protection, however, an equally thorough analysis as to whether the individual case requires a flexible interpretation of Fed. R. Evid. 501 has not consistently been conducted to confirm this interpretation.[65]

It is well settled that federal courts will permit the disclosure of peer review materials in federal question cases involving discrimination,[66] civil rights[67] and antitrust actions.[68] In these cases, the courts generally hold that the federal interest in discovery outweighs any interest in confidentiality, because otherwise the plaintiff may not be able to prove a valid claim.

Federal court opinions are split in actions involving the Federal Tort Claim Act (FTCA).[69] Here, where Congress established a forum in which liability claims, such as medical malpractice, can be pursued against the government in accordance with local state law, the Supreme Court has held that the language of the FTCA "assimilates into federal law the rules of substantive law of the several states."[70] Certain federal courts have interpreted this to mean, "federal law still supplies the 'rule of the decision' under Fed. R. Evid. 501 and state privilege law does not apply to FTCA cases."[71] In *Syposs v. United States*, the court did not find a peer review privilege in 42 U.S.C. § 11137(b)(1) and relied on the finding in *University of Pa. v. EEOC* that there was no federal common law self-analysis privilege.[72]

On the other hand, other federal courts have applied a flexible approach as to Fed. R. Evid. 501 and concluded that Congress intended state medical peer review privileges to apply. These courts support the application of the self-critical analysis privilege.[73] In *Weekoty v. United States*, the court noted that forty-six states and the District of Columbia had laws prohibiting the disclosure of peer review material and stated that "the nearly unanimous state legislative recognition of the self-critical analysis privilege in the medical peer review context confirms the appropriateness of recognizing the privilege in this forum."[74]

Federal courts, sitting in diversity jurisdiction, have permitted a peer review privilege under state law in all cases involving medical malpractice.[75] Two of these cases

65. *See e.g.*, 169 F.R.D. 550.

66. *See e.g.*,Virmani v. Novant Health Inc., 259 F.3d 284 (4th Cir. 2001)(racial discrimination); Mattice supra note 21 (ADA discrimination in employment); Johnson v. Nyack Hosp., 169 F.R.D. 550 (S.D.N.Y. 1996)(racial discrimination); Robertson v. Neuromedical Ctr., 169 F.R.D. 80 (M.D. La. 1996)(ADA action); Marshall v. Spectrum Medical group, 198 F.R.D. 1 (D. Me. 2000)(ADA action).

67. *See e.g.*,LeMasters v. Christ Hosp., 791 F. Supp. 188 (S.D. Ohio 1991)(Title VII action based upon alleged termination of staff membership after participation in EEOC proceedings and sex discrimination); Smith v. Alice Peck Day Memorial Hosp., 148 F.R.D. 51 (E.D. N.H. 1993)(civil rights § 1981 action); Leon v. The County of San Diego, 202 F.R.D. 631 (S.D. Cal. 2001)(civil rights § 1983 action with pendant state claim for medical malpractice); Krolikowski *supra* note 23 (Title VII action).

68. *See e.g.*, Memorial Hosp. For McHenry County v. Shadur, 664 F.2d 1058 (7th Cir. 1981); Swarthmore Radiation Oncology, Inc. v. Lapes, 1993 U.S. Dist. LEXIS 17555, 1993 WL 517722 (E.D. Pa. Dec. 1, 1993); Nilavar *supra* note 22; Wei *supra* note 17; Pagano, *supra* note 15; Salamon v. Our Lady of Victory Hosp., 202 U.S. Dist. LEXIS 4207 (W.D.N.Y. Feb. 12, 2002); Teasdale v. Marin Gen. Hosp., 138 F.R.D. 691 (N.D. Cal. 1991).

69. 28 U.S.C. § 2671 et seq. (2003).

70. Feres v. United States, 340 U.S. 135, 142 (1950).

71. *See e.g.*, Feres *supra* note 71; Menses v. United States Postal Service, 942 F. Supp. 1320, 1321 (D. Nev. 1996); Galarza v. United States of America. 179 F.R.D. 291 (S.D. Cal. 1998); Young v. United States, 149 F.R.D. 199, 202 (S.D. Cal. 1993)(the legislative history of Fed. R. Evid. 501 supports the conclusion that Congress intended federal privilege law to apply to claims brought under the FTCA); Syposs v. United States, 179 F.R.D. 406 (W.D.N.Y. 1998); Tucker v. United States, 143 F. Supp. 2d 619 (S.D.W.Va. 2001);

72. 179 F.R.D. at 410.

73. *See e.g.*, Weekoty *supra* note 15 (the self-critical analysis privilege requires the confidentiality of its products); Mewborn v. Heckler, 101 F.R.D. 691 (D.D.C. 1984)(finding that the availability of raw factual data is sufficient for the purposes of discovery and the results of peer review are privileged); Whitman v. United States, 108 F.R.D. 5 (D. N.H. 1985)(finding a privilege but not enforcing it due to procedural waiver); Gillman v. United States, 53 F.R.D. 316 (S.D.N.Y. 1971)(holding that an administratrix was not entitled to government reports made by a board of inquiry established to conduct an investigation into the death of decedent); *see also* Virmani *supra* note 67 (discussing the application of peer review privilege in a malpractice action).

74. 30 F. Supp. 2d at 1346-47.

75. *See e.g.*, Bredice *supra* note 15(provided a qualified privilege for peer review material unless extraordinary circumstances warranted discovery); Armstrong v. Dwyer, 155 F.3d 211 (3rd Cir. 1998)(court held federal statute 42 U.S.C. § 1320 covering Professional Peer Review Organizations expressly barred disclosure); Laws v. Georgetown University Hosp., 656 F. Supp. 824 (D. D.C. 1987)(qualified privilege if actual raw data is available to plaintiff following Bredice); Morse *supra* note 18(state law privilege applied to state law claim).

have been criticized by other courts for two principle reasons.[76] First, the seminal case of *Bredice v. Doctor's Hospital* is criticized because it was decided prior to the most recent enactment of Fed. R. Evid. 501. This criticism reflects a restrictive view of Fed. R. Evid. 501 and ignores the dicta in *Jaffee* that courts have the flexibility to fashion equitable resolutions.

Second, both *Bredice* and *Laws v. Georgetown Univ. Hosp.* are criticized because they involved medical malpractice cases sited in the District Court of the District of Columbia, which in a different jurisdiction would have been heard in a state court applying the state law of privileges. These criticisms ignore the rationale applied by the courts that confidentiality of peer review materials is necessary to develop the peer review process and achieve the public interest in the improvement of healthcare.[77]

Moreover, these criticisms do not address the difficulty that arises where state medical malpractice actions attach with federal claims, such as in actions involving the Emergency Medical treatment and Active Labor Act (EMTALA),[78] the Employment Retirement Income Security Act (ERISA),[79] as well as 42 U.S.C. § 1983 civil rights actions.[80] In *Leon v. The County of San Diego*, a federal jurisdiction case, the court permitted disclosure of peer review materials for the purposes of plaintiff's civil rights claim, and issued a protective order limiting its use to support the pendent state malpractice action.[81]

The use of a protective order in these types of cases allows the court to fashion a remedy which satisfies the federal interest in facilitating discovery to allow the plaintiff to pursue her federal cause of action while protecting peer review materials from use in litigating medical malpractice claims. As discussed above, *Jaffee* authorizes federal courts to define new privileges under the federal common law where the privilege promotes an interest that outweighs the need for probative evidence. Courts which have been critical of a peer review privilege, or reluctant to grant a privilege due to concerns over satisfying the federal interests of discovery, can achieve a more equitable resolution by following this path.

The federal common law peer review privilege continues to be criticized and developed in federal courts. Privileges have been recognized where plaintiffs are not prohibited from pursuing their federal claims or denied access to raw actual data for purposes of their malpractice actions. This is particularly important as an increased amount of aggregate health information is made available through data collection and automated processing.

Since Congress has not expressly acted to create a federal privilege for peer review materials, the burden is on the federal courts to consider the dicta in *Jaffee*, and seek equitable resolutions to conflicting demands for information by balancing plaintiff's need for actual data with defendant's interest in maintaining a confidential review process. Otherwise, medical care providers will have a disincentive to analyze raw data in hopes of improving medical care delivery when the results of this study may be made available to the plaintiff's bar for the development of litigation strategies. The federal courts are not prohibited from acting in this area, although they remain reluctant to do so.

Similarly, the federal courts will eventually have to address what limitationsare available as to the use and disclosure of identifiable or de-identified data made available to, and processed by, researchers, since HIPAA provides no express protection over the results of study. Furthermore, Congress must recognize that the courts are reluctant to provide protections in this sensitive area and it should act prospectively to insure that the federal interest in medical peer review is secured.

---

76. Nilavar *supra* note 22 at 603.

77. 656 F. Supp. at 826.

78. *See e.g.*, Gatewood v. Washington Healthcare Corp., 933 F.2d 1037 (D.C. 1991)(court found no viable federal cause of action under EMTALA and dismissed pendent state malpractice claim).

79. *See e.g.*, Cicio v. Does, 321 F.3d 83 (2d Cir. 2003)(medical malpractice claim not preempted by ERISA).

80. *See e.g.*, Leon *supra* note 68.

81. Leon *supra* note 68.

PART IV

The development and support for a peer review privilege in the states has continued during a time when the federal courts have largely disfavored privileges and Congress has only provided limited immunities.

State Statutory Efforts to Establish Medical Peer Review Privileges

States have created varying degrees of privileges and immunities in order to encourage peer review activities that are substantially, if not completely, in harmony in recognizing a medical peer review privilege.[82] The protections offered under these state statutes are not uniform, but generally, as in HCQIA, offer some limited immunity to members of the peer review committees from civil damages. Further, the majority of states extend this privilege to discovery of documents and provide for confidentiality of the information obtained in the peer review process.

State statutes restricting the use and disclosure of medical information tend to be either specific to (1) certain health care providers or (2) medical conditions for the purpose of public health reporting, leaving much information in the state health care system unprotected.[83] As noted above, although HIPAA provides a minimum floor for the protection of patient privacy, it does little or nothing to protect the confidentiality of peer review proceedings. As such, a decision such as the one made by the state of Hawaii to repeal its state privilege law and rely exclusively on the Federal Privacy Rule is misplaced and leaves many entities unregulated.[84]

In contrast to Hawaii, other states have compared their statutes with HIPAA regulations and created "preemption charts" which reflect where HIPAA preempts state law and where state law supercedes HIPAA.[85] For example, the New York State Department of Health has concluded that "none of the peer review information which must be kept confidential under Public Health Law § 2805-m is part of an individual's designated record set under HIPAA and, therefore, the New York State law supercedes HIPAA."[86]

As indicated above, state law will be protected whenever it is more stringent than the HIPAA requirements. Since HIPAA fails to adequately address the protection of peer review documents most, if not all, of the state laws will be more stringent and thus survive HIPAA preemption.

---

82. *See, e.g.*, 735 Ill. Comp. Stat. 5/8-2101-2102 (2003) (providing that all information obtained "shall be privileged, strictly confidential and shall be used ... [for] evaluation and improvement of quality care, or granting, limiting or revoking staff privileges ... [and] shall not be admissible as evidence, nor discoverable in any action of any kind"); La. Rev. Stat. Ann. 13:3715.3 (West 2003) (providing confidentiality and privilege of peer review committee records, except when requested by physician whose staff privileges are affected); Md. Code Ann., Health Occ. 14-501(d) (2003) (providing statutory exception for actions initiated by physicians aggrieved by committee decision to obtain records for use in that physician's challenge to peer review conclusions); N.Y. Pub. Health Law § 2805-m (McKinney 2003) (providing similar exemption for discovery); N.C. Gen. Stat. 131E-95(b) (2003) (granting civil immunity to members of medical review committee and privilege from discovery or introduction into evidence of any records and material committee produces provided that process is performed without "malice or fraud"); Fla. Stat. 395.0193 (2003) (providing good faith participants with immunity from retaliatory suits and federal antitrust suits); Pa. Stat. Ann. tit. 63, 425.4 (West 2003) (stating that "proceedings and records of a review committee shall be held in confidence and shall not be subject to discovery or introduction into evidence in any civil action against a professional health care provider arising out of the matters which are the subject of evaluation and review by such committee"); Tex. Rev. Civ. Stat. Ann. art. 4495 5.06 (Vernon 2003) (allowing physician who is denied privileges to obtain copy of final decision and "except as otherwise provided ... all communications made to a medical peer review committee are privileged"); Va. Code Ann 8.01-581.17 (Michie 2003) (providing privilege and freedom from discovery with respect to all "proceedings, minutes, records or reports" of any "medical staff committee, utilization review committee, or other committee ... that provides a centralized credentialing service, together with all communications, both oral and written, originating in or provided to such committees or entities"); Ga. Code Ann. 31-7-143 (2003) (protecting committee records from discovery); Oh. Code Ann. 2305.251 (2003)(prohibiting discovery of peer review records); Cal. Evid. Code § 1157 (2003)((granting immunity from discovery to records of hospital peer review activities); Ala. Code 22-21-8 (2003)(medical self-critical analysis privilege).

83. Pritts, Joy L., Developments and Trends In The Law: Altered States: State Health Privacy Laws and the Impact of the Federal Privacy Rule, 2 Yale J. Health Pol'y L. & Ethics 325 (Spring 2002).

84. *See* 2001 Haw. Session Laws 244.

85.*See* http://www.health.state.ny.us/nysdoh/hipaa/ hipaa_preemption_charts.htm (last visited May 19, 2003).

86. *Id.*

The Fourth Circuit Court of Appeals Decision in *Virmani v. Novant Health Inc.* Sets Forth an Argument for the Application of the State Peer Review Privilege

In *Virmani* the court analyzed the split between other federal and state courts in determining whether to apply the North Carolina statutory peer review privilege.[87] That privilege, similar to many other states, grants privilege from discovery of any records and material a peer review committee produces, provided that the peer review process is performed without "malice or fraud."[88]

Notably, the *Virmani* court supported a flexible interpretation of Fed. R. Evid. 501. While agreeing with the holdings in state court cases, the *Virmani* court found that the state privilege was not applicable in a discrimination suit because of the overwhelming federal interest in ferreting out discrimination. The court opined, however, that the privilege may be applicable in medical malpractice actions.[89]

The court reasoned that in a discrimination case, the claim arises from within the peer review proceedings. This establishes a need in discrimination cases for plaintiff's access to peer review records. On the contrary, in a malpractice action the claim occurs from events outside of the proceedings. Therefore, preventing the plaintiff's access to peer review records will not impact greatly on the ability of the plaintiff to obtain necessary evidence.[90] Thus, the *Virmani* court reinforced the argument for finding a medical peer review privilege in pendent medical malpractice actions in federal courts by following the reasoning of the Supreme Court in *Jaffee* and using a flexible application of Fed. R. Evid. 501. *Virmani* also exemplifies the inconsistency in the application of state peer review privilege when a case is heard in federal court rather than state court. Here the court recognized that the North Carolina statute would have been applied if the case were heard in North Carolina state court, but denied the application of the state statute because the privilege would have limited disclosure in this discrimination matter.

PART V

The absence of a federal self-critical analysis privilege, together with an uneven set of state laws, has serious ramifications for medical care providers. This is further complicated by the lack of federal protection afforded by, and potential disclosure of data under, HCQIA and HIPAA.

Attorneys representing clients in federal courts must argue that Fed. R. Evid. 501 is a flexible rule, pursuant to the interpretation provided by the Supreme Court in *Jaffee*, and not a restrictive rule as certain courts have held. Applying a flexible balancing approach, federal courts can recognize that neither HCQIA nor HIPAA prohibits the federal courts from applying state privilege laws, that health care has long been the province of the states and that the states have uniformly recognized the need for a peer review privilege.

Counsel should encourage federal courts to follow the rationale of the *Bredice*, *Laws* and *Virmani* courts and provide state statutory peer review privilege protection to materials prepared as part of a medical facility's self-critical analysis process, at a minimum, in any pendant medical malpractice actions in federal court.

87. Virmani *supra* note 67.
88. N.C. Gen. Stat. 131E-95(b).
89. 279 F.3d at 291.
90. *Id.*

European Data Protection: Impact on U.K.-U.S. Data Transfers

By Ian MacDonald and Julia Graham

Ian MacDonald graduated with an LLB from Dalhousie University (Nova Scotia) in 1990. Having qualified in Toronto with Davies Ward & Beck, where he became a partner in 1994, he then re-qualified as a UK solicitor and joined the London firm of Arnander Irvine & Zietman. MacDonald has been a partner in the London office of Shook Hardy & Bacon since 2002 and has worked extensively on corporate security and commercial transactions as well as undertaking forensic legal work on commercial fraud matters.

Julia Graham studied law at the University of Toronto, graduating with an LLB in 1996. She is qualified as a solicitor in both the UK and Canada and works on a range of non-contentious commercial matters, with a particular focus on copyright, trademarks, technology licensing, data protection and e-commerce.

Personal data has become an increasingly valuable commodity as e-commerce expands. Its use in Europe is regulated by the Data Protection Directive[1] (the "Directive") which has been implemented throughout the European Economic Area[2] and was brought into effect in the UK by the Data Protection Act 1998 (which came into force in March 2000). Crucially, from the perspective of an American company with U.K. (or any European) operations, the Directive significantly affects the ability of the company's European affiliates or distributors to transmit consumer data back to headquarters.

This paper will outline the key provisions of the Directive before considering the various ways in which Anglo-American data transfers can be legally undertaken, including the solution which has been fashioned between the European Commission and the U.S. government, the so-called "Safe Harbor" self-certification system.

Purpose and Application of the Directive

In contrast to the more laissez-faire approach adopted in the United States, the Directive introduced an entire regulatory regime designed to (i) protect the rights and freedoms of individuals, particularly in the context of processing of personal data, and (ii) facilitate the free flow of personal data within the EU. The Directive governs all forms of processing of personal data, including the collection, storage, disclosure, updating and destruction of data, and applies to "data controllers" (the parties controlling the purpose and manner of the processing) as well as the "data processors" acting on their behalf. Personal data is defined as data that allows individuals (referred to as "data subjects") to be identified personally, as opposed to aggregated anonymous data.

Core Principles

Both the Directive and the Data Protection Act 1998 establish eight core principles that govern the collection, processing and use of personal data. The principles are:

1. Properly, it is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2. The EEA currently comprises the 15 member states of the European Union (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden and the UK) plus Liechtenstein, Norway and Iceland.

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Directive (and national implementing legislation).

7. Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Additional Requirements

Personal data can be collected and processed only if (i) the subject has unambiguously consented; or (ii) if the processing is necessary to meet a contractual obligation to which the subject is a party; or (iii) if it is necessary to meet a legal or public interest obligation. Where data has been collected for one purpose, it cannot be used for another without the consent of the subject. Certain types of data - relating to medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health or sex life - are considered "sensitive personal data" and require the **explicit** consent of the data subject before they are processed.

In addition, the requirement that personal data be processed in accordance with the rights of data subjects means that the subject has the right to know who is collecting and processing the data, the purposes of the processing and the recipients of the data. The subject also has a right of access to the data and the right to require the correction of data which is incomplete or inaccurate.

International Transfers of Data

Because the Directive has ensured a uniform degree of protection for personal data throughout the European Economic Area, the movement of personal data within the EEA is unrestricted, as long as data controllers register with the data protection registries where they are operating and otherwise comply with the laws of the member states where they are established. However, in order to ensure that data controllers do not avoid European regulatory requirements simply by transferring data outside the EEA, the Directive restricts the transfer[3] of personal data to countries outside the EEA.

As expressed by the eighth data protection principle, data can be transferred only to non-EEA countries that ensure "an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." The difficulty lies in identifying whether a non-EEA country ensures an adequate level of protection for this purpose. The Directive authorises the European Commission to publish findings as to the adequacy (or lack thereof), but since the Commission has opted only to publish a "white list" of approved countries, and has listed only Switzerland, Hungary, Argentina and Canada (in part), there remains considerable uncertainty in relation

3. It is important to distinguish the "transfer" of data to a country from the "transit" of data through a country. A "transfer" requires personal data to be held as such (as opposed to in aggregated anonymous form) both before and after its completion. While a transfer is regulated under the eighth data protection principle, the mere transit of data is not.

to transfers to other non-EEA countries. Notably, the Commission has not designated United States as a country that provides "adequate" protection for personal data.

Safe Harbor

To avoid the severe disruption of data flows that this position threatened to cause, in July 2000 the Commission and the U.S. government reached a compromise in the form of the "Safe Harbor" scheme which, notwithstanding rejection by the European Parliament, became operational on 1 November 2000.

Participation in the Safe Harbor scheme is voluntary, and involves a self-certification process. To receive the benefits of the scheme, an organization must either self-certify to the U.S. Department of Commerce (on an annual basis) that it will abide by the Safe Harbor requirements, or be a member of a self-regulatory organization that so certifies. In either case, U.S. companies that comply with these requirements will be deemed, for the purposes of the Directive and relevant national implementing legislation, to provide adequate protection for personal data.

In brief, the Safe Harbor requirements are as follows:[4]

Notice: An organization must inform individuals about (i) the purposes for which it collects and uses information about them, (ii) how to contact the organization with any inquiries or complaints, (iii) the types of third parties to which it discloses the information, and (iv) the choices and means the organization offers individuals for limiting the use and disclosure of their information. This notice must be provided in clear and conspicuous language, ideally when individuals are first asked to provide personal information to the organization or as soon as possible thereafter, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party.

Choice: An organization must allow individuals to choose whether to have their personal information (i) disclosed to a third party, or (ii) used for a purpose that is incompatible with the purpose(s) for which it was originally collected or any purpose(s) subsequently authorized. For sensitive information (corresponding to "sensitive personal data" in Europe), specific consent must be given to any such disclosure or use. In other cases, individuals must be provided with clear, conspicuous and affordable mechanisms by which to opt out of such disclosure or use.

Onward Transfer: To transfer information to a third party acting as an agent, an organization must verify that the third party complies with the Safe Harbor requirements or is subject to the Directive or another adequacy finding. As an alternative, the organization must enter into a written agreement requiring such third party to provide at least an equivalent level of privacy protection. If the organization complies with these requirements, as a general rule it will not be held responsible if the third party processes the information in a way that is contrary to any restrictions or representations (although in certain cases exceptions may apply).

Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect against loss, misuse, disclosure, alteration or destruction of, or unauthorized access to, such information.

Data Integrity: Personal information must be relevant for the purpose(s) for which it is to be used. An organization may not process personal information in a way that is incompatible with these purpose(s) or any purpose(s) subsequently authorized by the individual and, to the extent necessary for those purpose(s), should take reasonable steps to ensure that data is accurate and complete.

Access: Individuals must have access to personal information held about them by an organization and be able to correct or delete

4. Source: Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 21, 2000, available at: http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm.

any inaccurate information, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Enforcement: Organizations must have in place (i) readily available and affordable independent recourse mechanisms to facilitate the investigation and resolution of individual complaints and disputes, (ii) procedures that will allow the organization's compliance with the Safe Harbor requirements to be monitored, and (iii) systems to ensure that problems arising out of compliance failures are remedied. Whatever the dispute resolution/compliance system, it must ensure that sufficiently severe sanctions are imposed for non-compliance with the Safe Harbor requirements.

In general, Safe Harbor functions as a self-regulatory scheme, with organizations satisfying their obligations with respect to enforcement by such methods as (i) voluntarily complying with government supervisory authorities, (ii) committing to cooperate with European data protection authorities, or (iii) complying with a private sector developed privacy seal program (provided such program incorporates and satisfies the Safe Harbor requirements). Private sector regulation must then be backed up as needed by government enforcement of federal and state laws prohibiting unfair or deceptive acts or practices, with persistent failures to comply resulting in loss of certified Safe Harbor status for the organization in question.

One of the perceived advantages of the Safe Harbor scheme is, thus, that all enforcement takes place in the U.S., under U.S. law. However, the requirement for effective government sanctions to back up self-regulation has meant that only organizations that are regulated by the Federal Trade Commission or the Department of Transportation (with respect to air carriers and ticket agents) can participate in the scheme, since only these bodies have committed to take enforcement action in response to non-compliance with Safe Harbor. Notably, therefore, organizations operating in the financial industry are not eligible to sign up to the scheme. In other cases, eligible organizations have been reluctant to sign up in light of the perceived cost and difficulty of compliance.

Self Assessment of Adequacy

Notwithstanding that the European Commission has not approved the United States as providing adequate protection for personal data, the export of data from the U.K. to the U.S. may be permissible on alternate grounds. In particular, because the Directive provides that the adequacy of protection in relation to any given transfer of data or set of transfers is to be determined "in light of all circumstances surrounding the data transfer", the U.K. Data Commissioner (the "Commissioner") takes the view that a data controller is free to draw its own conclusions as to adequacy. According to the Commissioner, a country can be considered to provide adequate protection for a particular transfer or set of transfers if the level of protection in the particular case "is commensurate with the potential risks to the rights of the data subjects."[5]

In making this determination, a U.K. data controller will need to take various factors into account. Sensitive personal information will, for example, require more stringent protections to be in place in the country to which the data is to be exported. The country of origin of the data at issue may also be relevant, particularly where the data actually derives from a country outside the EEA where it would not originally have been entitled to the same protection as it will have acquired by virtue of having entered the EEA. The final destination of the data will similarly be relevant. Other factors will include the purposes for which and the period during which the data are intended to be processed, the law in force in the recipient country and any security meas-

5. Source: U.K. Information Commissioner, International Transfers of Personal Data: Advice on Compliance with the 8th Data Protection Principle at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.

ure taken in respect of that data in the recipient country (e.g., encryption).

In the Commissioner's view, certain types of data transfer are more problematic than others[6]. Transfers to a third party with whom the data controller remains in an ongoing relationship tend to be less risky than, for example, transfers that amount to a sale of data to an unrelated third party. In fact, the Commissioner has indicated that in certain circumstances, a presumption of adequacy can be made. Thus, in the case of a transfer within a multi-national company or group of companies, or a transfer between lawyers or accountants in relation to clients whose affairs are international in scope, or a transfer to a data processor controlled by the data exporter, personal data will be considered adequately protected as long as there exist adequate controls and procedures for ensuring the transferred data is given proper treatment.

The Commissioner recommends that, before effecting a transfer to an "inadequate" country, a data controller consider certain general criteria (principally relating to the nature and purpose of the transfer), as well as legal criteria (relating primarily to the laws of the jurisdiction to which the data will be transferred). Once the risks involved in the transfer have been assessed in this way, the data controller can determine (i) whether contractual or self-regulatory measures are necessary to ensure that the transferred data receives adequate protection, and (ii) assuming that such measures are required (as they will be in most cases), how to implement measures that will ensure an appropriate degree of protection for the transferred data. In the case of a multi-national company or group of companies, suitable measures may take the form of company policies or codes of conduct, but in other cases binding contractual provisions will have to be put in place.[7]

However, because no mechanism exists for pre-clearing arrangements made on the basis of a self-assessment, self-assessment remains potentially risky for data controllers seeking to export data from the U.K., particularly in cases where no presumption as to adequacy arises. In addition, and as noted by the Commissioner, it may not be efficient in terms of either time or resources for data controllers to have to assess every single data transfer they propose to undertake.

Standard Contractual Clauses

To reduce some of the legal uncertainty associated with international data transfers, the European Commission introduced a series of standard contractual clauses that can be incorporated into contracts providing for the transfer of data outside the EEA.[8] Although data controllers are not obliged to use these model clauses, any transfer of personal data made on the basis of such terms will be deemed to comply with the eighth data protection principle, provided the parties to the relevant contract fulfil their contractual obligations.

Data Controller Clauses: The first set of standard contractual clauses is for use by data controllers exporting data to other data controllers. The obligations imposed by the model clauses on the data exporter include confirming that it has complied with national data protection legislation prior to the transfer and notifying the data subjects if sensitive personal data are to be transferred. Although data exporters may not be able to provide such notices where large transfers

6. U.K. Information Commissioner, *The Eighth Data Protection Principle and Transborder Data Flows* July 1999, at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.

7. The EU Article 29 Working Party - consisting of representatives of the data protection authorities in EU member states - has recently made a proposal that, if adopted, would facilitate the use of binding corporate rules to govern intra-corporate transfers of personal data. According to the proposal, if a multi-national corporation can show that it has in place a code of corporate conduct meeting certain specified criteria (these relate principally to the binding nature of such code, its legal enforceability and the procedures the corporation has implemented for ensuring compliance), any personal data transferred from one entity in the corporate group to another outside the EEA will be deemed to be adequately protected. *See* Working Document: Transfers of personal data to third countries; Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted 3 June 2003, available at www.europa.eu.int/comm/privacy.

8. *See* Decisions 2001/497/EC and 2002/16/EC, available on the Commission's website at http://europa.eu.

of data are involved, it is arguably the importing data controller who is made subject to the more onerous obligations. In general, the data importer must comply with the eight European data protection principles (although in certain cases full compliance may not be necessary) and accept any directions given by the national data protection authority (or "supervisory authority") established in the jurisdiction of the data exporter. Both parties are obliged to make a copy of model clauses available to data subjects upon request and to assist with compliance queries.

In addition, the model clauses render the data exporter and importer jointly and severally liable for any breach of their obligations and specifically designate data subjects as third party beneficiaries of the contracts who can therefore sue for any breach. As a result, any data exporter or importer is potentially liable for a failure by the other party to the contract to fulfil its obligations. While this solution has the advantage of protecting data subjects, in reality it is likely to be acceptable to data importers and exporters only where they are related companies.

Data Processor Clauses: The model clauses for use by data controllers contracting with data processors are similar to those prescribed for contracts between data controllers. But whereas an importing data controller is required to comply generally with the eight data protection principles, an importing data processor must agree to process the data in accordance with the data exporter's instructions and to implement certain agreed technical and organizational measures to protect the data. In exchange, the data exporter must warrant that its proposed security measures are appropriate, despite the fact that in many cases the data exporter will be relying on the data importer's expertise in this regard.

Even more controversially, the model clauses impose liability on the data processor for any damage suffered by data subjects in cases where the exporting data controller has "disappeared factually" (whether through bankruptcy, winding up or otherwise). Although the drafters of the relevant clause apparently intended to hold the data processor responsible only for damage arising out of the data processor's breach, ambiguous wording could also render the data processor liable for damage caused by the data controller.

Perhaps for the reasons suggested above, the Commission's standard contractual clauses have not been as widely adopted as was hoped. Nonetheless, if they are not already, they appear set to become the de facto standard against which all contracts relating to overseas transfers of data will be assessed and for this reason are relevant to all parties contemplating the transfer of personal data outside the EEA.

Permitted Derogations

Consideration must also be given to the exceptions to this principle that are set out in the Directive and reflected in the Data Protection Act 1998. For example, the transfer of personal data to countries without an "adequate level of protection" can take place: (i) with the consent of the data subject; (ii) when it is necessary for the performance or conclusion of a contract with or on behalf of the data subject; (iii) when legally required on public interest grounds; or (iv) in order to protect the "vital interests" of the data subject.

Of these exceptions, the first may be the most useful, but the consent of the data subject must be unambiguous, freely given and informed. In some cases, the requirement for consent to be "informed" may oblige data controllers to advise data subjects of the potential risks involved in the transfer of their data outside the EEA. In addition, consent must be "signified," and so should not be inferred from mere failure to object. As a result, reliance on consent as the legal basis for a transfer may not always be possible, particularly in cases involving the transfer of large existing databases or the sale of direct marketing lists.

Conclusions

Data controllers can export personal data from Europe to the U.S. in compliance with the Safe Harbor scheme, on the basis of a self-assessment of adequacy made by a U.K. based data controller, by using the European Commission's model contractual clauses or by relying on one of the exceptions provided for under European law. In any of these cases, both the party transferring the data and its recipient should give careful consideration to the circumstances surrounding the transfer, and in particular any factors that might jeopardize the security of the data being transferred and the protective measures that should or must be implemented. While the cost and inconvenience of doing so may seem high, it should be borne in mind that, as data protection authorities become increasingly active in enforcement, and individuals increasingly protective of their personal information, the potential cost of non-compliance is rising.

The Privacy Project II

Managing Privacy and Security Risks in Your Business: Are You Properly Protected?

By Kathy J. Maus, Michael G. Haire, Jr. and Emily Freeman

As the global concerns over security and personal privacy increase, opinion and policy continue to generate legislation defining and expanding an individual's right to privacy. Each codified expansion of privacy simultaneously creates new corresponding duties and obligations. Often these duties and obligations impact businesses in unanticipated or even unintended ways, creating unknown liability and litigation traps for the uninformed. With the advent of civil liability and criminal penalties imposing jail time and fines reaching hundreds of thousands of dollars, the stakes are high indeed.

For the business owner, no business decision is without risk. By making use of state of the art security models and technologies, companies have been able to reduce costs, improve the quality of products and services, and increase profits. Even after all cost-effective safeguards are in place, however, security and privacy risks still remain and cannot be reduced to zero, based upon the current state of technology, people and processes controls. The organization must continue its business notwithstanding the remaining risks.

This paper will address not only the recent developments in the areas of security and personal privacy, but the coverage concerns businesses may encounter. By better understanding the relationship between the expansion of personal privacy and the associated obligations, businesses are better informed, prepared and protected. Also, innovative insurers have recognized these risks and assistance is available to alleviate some of the concerns.

Although popular opinion may ascribe our rights to privacy to the U.S. Constitution, no such right is found there. Instead, such a right has been judicially created, based in the Fourth Amendment. The Fourth Amendment provides as follows:

> Amendment IV. Search and Seizure - The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In the 1960s, the United States Supreme Court revised its approach to the Fourth Amendment, recognizing an individual's right to privacy against unreasonable searches and seizures. The Court employed a balancing test in which it weighed the government's powers and desire to search, against the potential for abuse of discretion

IADC member Kathy J. Maus is a partner in the state-wide law firm of Butler Pappas Weihmuller Katz Craig LLP, practicing in its Tallahassee office. She heads its third-party liability, first and third party automobile coverage, and extra-contractual litigation departments in that office. She graduated with honors from FSU College of Law in 1991.

Michael G. Haire, Jr. is an associate with the Tallahassee office of Butler Pappas, joining the firm in 2001. Mr. Haire practices in the property coverage department, primarily focusing on first party fire and theft cases.

Emily Q. Freeman, ARM, AU, is Vice President-Western Region and Executive Director of Consulting for American International Group (AIG) eBusiness Risk Solutions. She has been a key drafter of cyberspace insurance products and a senior consultant for e-business risk management. The views and opinions expressed are those of the author and do not necessarily reflect those of American International Group, Inc. or its subsidiaries, business units, or affiliates.

by police against an individual's privacy.[1]

Most states currently protect an individual's right to privacy by permitting third-party claims resulting from the disclosure of personal information. Importantly, in the insurance claims arena, an insurer must weigh its right and duty to investigate a claim (including gathering past claims history, medical records and surveillance on a claimant) against the claimant's/insured's right of privacy. From the individual business/insured's standpoint, coverage for a third-party breach of privacy claim way not exist or coverage might be denied. The next section will explore several examples of permitted privacy claims and some examples of insurance coverage defenses that recent history shows may be asserted.

1. Potential Claims

As noted above, in the third-party claim setting, where invasion of privacy is alleged, special concerns arise. The common law torts of negligent or intentional infliction of emotional distress for privacy violations are based on one or more of the four following elements:

1. Unreasonable intrusion upon Plaintiff's seclusion.
2. Public disclosure of private facts.
3. Publicity which places one in a false light.
4. Violation of a privacy statute.

Trespass, defamation, bad faith from invasion of privacy and interference with business relationships are also in this category. On the immediate horizon relating to security, a growing concern is the potential for allegations of negligence in failing to prevent the spreading of a computer virus that results in lost or damaged data. Such claims will certainly be based on improper, inaccurate, and/or incomplete virus software, virus protection policies and implementation.

Usually, a standard Commercial General Liability (hereinafter "CGL") policy will not protect the alleged "invader." Whether searching for coverage under the "bodily injury," "property damage," "personal injury" or "advertising injury" sections of the traditional CGL policy, such claims will likely be denied.

Where invasion of privacy claims are asserted, most insureds look to the definitions and insuring agreements for personal or advertising injury under their policies. For example, in the standard CGL coverage form, CG 00 01, personal injury is defined as "(1) oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services, and (2) oral or written publication of material that violates a person's right of privacy." Advertising injury is defined as "(1) oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services, (2) oral or written publication of material that violates a person's right of privacy, (3) misappropriation of advertising ideas or style of doing business, and (4) infringement of copyright, title, or slogan." In this day and age, of particular concern is where internet or electronic communications are the source of the privacy invasion, because "publication" must occur to trigger coverage.

Privacy violations on the internet can occur when private information is sold to a few businesses. "Publishing," or making private information public in this context is similar to the standard defamation determinations, i.e., the information is made public when it is communicated to at least one person. However, a different standard applies with e-commerce. "Publication" in the e-commerce environment usually means more than disclosure to just one-or even a few.[2] If there is no publication, either

1. Three landmark cases stand out in the development of the right to privacy as interpreted by the U.S. Supreme Court. Katz v. United States, 389 U.S. 347 (1967); Camara v. Municipal Court, 387 U.S. 523 (1967); and Terry v. Ohio, 392 U.S. 1 (1968).

2. The complexities and uncertainties regarding online publication issues and privacy are also revealed in trade-mark litigation. Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999). In Lane, a student, not employed by Ford, posted Ford's confidential documents and trade secrets on his Web site, disclosing photographs of unreleased products, blueprints, and other confidential information. The court *denied* plaintiff's motion for a preliminary injunction against the use, copying or disclosure of Ford's internal documents, holding that such an injunction would constitute an invalid prior restraint in violation of the First Amendment. *Id.* at 753-754.

because it is not required or because its scope is insufficient to constitute a "public publishing," then there may be no coverage because the policy terms have not been met.

In addressing whether claims arising under these provisions are covered, courts will weigh the facts and circumstances of a particular business, including the nature of activities in which the business *is generally engaged*. In *St. Paul Guardian Insurance Co. v. Centrum GS, Ltd.*,[3] (applying Texas law), the court considered whether a terminated employee's breach of privacy claim was covered under the insurance policy of the employer, a building owner/manager. After terminating the employee, the employer posted "wanted posters" including the photograph, name, home address, driver's license, automobile tag and Social Security numbers of the terminated employee. The insurance company argued that the claim was not covered because the privacy violation did not stem from the "business activity" of the insured. However, the Fifth Circuit held that the claim was covered because the insured's actions were "consistent with their business of owning and managing property."[4]

In another case involving the violations of privacy under Texas law, the court in *St. Paul Fire & Marine Ins. Co. v. Green Tree Financial Corp.*,[5] determined there was coverage for "rude and abusive" telephone calls made by a collection agency over an eight-year period.[6] The policy provided coverage for personal injury arising out of "written or spoken material made public which violates an individual's right of privacy."[7] The court disagreed with the insurer's argument that the pleadings did not specifically allege an invasion of privacy, holding that the factual allegations supported a cause of action for invasion of privacy under Texas law.[8]

The *Green Tree* decision illustrates a hesitancy in some courts to *preclude* coverage for torts based on invasion of privacy, even where publication has not actually occurred. Curiously, the 1998 CGL policy redefined "advertisement" to constitute *broad* dissemination, however, the word "publication" was not similarly redefined.[9] Therefore, if no advertising occurred, then the personal injury coverage section should be triggered. On the other hand, an advertising injury exclusion of which to be aware is the broadcasting exclusion for companies *in the business of advertising, broadcasting, or publication*: if a disclosure is deemed an advertisement made by an entity in the business of advertising, coverage is specifically excluded.

Such was the determination of the court in *American Employers' Insurance Co. v. DeLorme Publication Co., Inc.*[10] In *DeLorme*, the policy excluded coverage for advertising injury "arising out of ... [a]n offense committed by an insured whose business is advertising, broadcasting, publishing or telecasting."[11] The court held that the exclusion applied, but only because the insured was a "publisher" engaged in the business of publishing.[12]

An unresolved issue at this point is whether a website is an advertisement. That is, it remains unclear whether there is coverage for defamation, slander or injury resulting from the disclosure of private information through a website. This is particularly important for law firms, where many states' bar rules classify websites as advertisements.[13]

The 2001 CGL amended advertising injury exclusions to ensure it only provided exclusions for those in the primary, chief business of advertisement.[14] Accordingly, the intentional acts exclusion includes an intentional inclusion of privacy information

3. 283 F.3d 709 (5th Cir. 2001).
4. *Id.* at 714.
5. 249 F.3d 389 (5th Cir. 2001).
6. *Id.* at 394.
7. *Id.* at 393.
8. *Id.* at 394-95.
9. For additional discussion of potential litigation issues arising out of the 1998 CGL changes, *see* Matthew J. Schlesinger and Jason M. Silverman, *Insuring Privacy: Is Your Company Covered?*, 37 Tort & Ins. L.J. 1101, 1105-1107 (2002).
10. 39 F. Supp. 2d 64 (D. Me. 1999).
11. *Id*. at 72.
12. *Id.*
13. *See, e.g.,* Fla. St. Bar Rule 4 7.6(d) (2003).
14. For further discussion of the 2001 CGL changes impacting issues of advertising, *see* Robert H. Jerry, II and Michele L. Mekel, *Cybercoverage for Cyber Risks: An Overview of Insurers' Responses to the Perils of E Commerce*, 8 Conn. Ins. L.J. 7 (2002).

which appears to be a violation of the businesses' own privacy policy. Although an argument exists that data is not "tangible property," problems remain in the area of e-commerce. Damage can occur too easily and the potential audience can be unusually large. Additionally, reinsurers are pressuring insurers to exclude e-commerce or to place a small sub-limit on such coverage. Therefore, knowing your policy is the key in determining how to navigate these issues.

II. Regulatory Environment

As noted above, the legislature on both the state and federal levels are continuously addressing the right to privacy and creating more protections. Consequently, these same legislatures are creating additional liability traps.

1. Graham-Leach-Bliley (GLB) Act

A leading piece of legislation in this debate is the Graham-Leach-Bliley (GLB) Act of 1999.[15] Effective in November 1999, the GLB Act was primarily aimed at the banking industry. However, "financial institutions" as defined in the act include all businesses engaging in financial activities, including appraisal and insurance services.[16] Another element of the act is its impact on lending securities. The act permits insurance companies to affiliate with banks and permits "financial institutions" to share non-public customer information[17] with affiliates within the holding company.

Protections also exist against disclosure to non-affiliates. As of July 1, 2001, the act requires all financial institutions to disclose to each consumer with whom it does business the policies and practices for protecting private information. Such policies and practices must be provided at the time of engaging the relationship and at least annually thereafter.[18] The customers must be provided with an opt-out application.[19] Even if no information will be shared, the customer must receive the privacy policy. However, these provisions apply only to customers with a regular, continuing relationship.[20] In the case of an isolated transaction, such information is not required. Of course, if the business is anticipating that the customer will engage in regular business with them, the corporation's privacy policies must be shared. The act requires the remaining customers to get notice if the information is actually shared.

Thus, there are a total of three types of notices required by the act: initial, annual and opt-out to non-affiliates. The initial and annual notices require providing the following four categories of information: 1) category of customer information collected, 2) category of information disclosed, 3) category of affiliates and non-affiliates to whom disclosed, and 4) the company's policies and practices regarding security and confidentiality.[21]

Reserving the right to disclose to non-affiliate (opt-out to non-affiliates), requires providing the following five categories of information: 1) timely notice, 2) advice that he/she/it can opt-out, 3) a reasonable method to opt-out, 4) a reasonable time to opt-out, and 5) notice that the decision to opt-out is binding until revoked.

The act encourages all states to provide similar privacy protection as long as it is at least equal to those provided in the act

15. 15 U.S.C. §§6801, et seq., also known as the Financial Service Modernization Act of 1999.

16. Specifically, § 6809 of the Act defers to the definition contained in 12 U.S.C. §1843(k)(4)(B), which specifically identifies the following as activities that are financial in nature: "Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State."

17. The Act defines such non-public information as "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." 15 U.S.C. §6809(4)(A).

18. The Act defines a "consumer" as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." 15 U.S.C. §6809(9).

19. 15 U.S.C. §6809(b)(1).

20. Essential in determining the nature of the relationship is when the "customer relationship" actually begins. Accordingly, "in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services," the phrase "time of establishing a customer relationship" is defined as "the time of establishing the credit relationship with the consumer." 15 U.S.C. §6809(11).

21. 15 U.S.C. §6803(b)(1)-(4).

itself.[22] It is clear that broader and greater protections than those offered in the act will be upheld. The National Association of Insurance Commissioners (NAIC) has promulgated rules to guide state departments of insurance in preserving opt-out rights for financial products and an opt-in provision for health information.[23] These rules are known as the Privacy of Consumer Financial and Health Information Regulations.[24] Approximately forty-three states have adopted these rules in one form or another.[25] These regulations expand the GLB Act in at least four key areas. First, the definitions of "consumer" and "customer" create two protected classes to whom privacy protection must be provided: applicants, as well as, policyholders.[26] Second, the NAIC model regulation also extends to commercial lines insurance.[27] Third, the model regulation provides requirements for disclosure of nonpublic personal health information.[28] Fourth, the standards apply to all entities licensed under insurance laws, rather than only financial institutions.[29]

One recently positive way in which the GLB Act was applied was in *The Equitable Life Assurance Society v. Irving*, - So. 2d -, 2003 WL 22098021 (Miss. Sept. 11, 2003). The Equitable court, specifically confirming that insurers are deemed financial institutions under the Act, held that an insurer may not be compelled to release its customer's private information without their consent. In that case, the plaintiff successfully obtain an order from the trial court which required the insurer to release a listing of all policy holders who purchased "vanishing premium" policies. The purpose of plaintiff's request for such an order was to permit plaintiff to demonstrate a pattern and practice of the insurer at issue in that case. Importantly, however, the Mississippi Supreme Court, applying this federal law, held as follows:

> The intent of the GLBA is to protect the customers of financial institutions from invasions of their privacy. Part of the purpose of this Act was to stop solicitations generated by customer lists, and this would include solicitation by an attorney to be a witness or for any other purpose. Thus, the GLBA preempts the issuance of the circuit court's order.

As such, the insurer was protected from producing these lists as was the insurers' customers.[30]

22. 15 U.S.C. 6807(b).

23. *NAIC's Priv. of Cons. Fin. and Health Info. Reg.* No. 672-1 §§2-3 (NAIC 2000).

24. *Id.*

25. *See* Ala. Ins. Dept. Reg. 122 (2000/2001); Alaska Admin. Code Title 3 §§ 21.06.05 to 21.06.749 (2001); Alaska Stat. § 21.36.162(2001); Ark. Ins. Rule & Reg. 74 (2002) SB 286 (2001); Cal. Admin. Code Title 10 §§ 2689.1 to 2689.24 (2002); Colo. Admin. Ins. Reg. 6 4 1(2000/2001); Conn. Admin. Code Title 38a 8 105 to 38a 8 123 (2002); Del. Ins. Reg. 84 (2001); Del. Code Ann. Title 18 § 535 (2001); D.C. Regs Title 26 § 3600.1 to 3614 (2000), Act 13 444 (2000); Fla. Admin. Code §§ 4 128.001 to 4 128.024 (2001); Fla. Stat. § 626.9651 (2001); Ga. Admin. Comp. Ch. 120 2 87 (2001); Hawaii Rev. Stat. §§ 431:3A 101 to 431:3A 504 (2001); Idaho Ins. Regs. 48 (2001); Ill. Admin. Reg. Title 50 §§ 4002.10 to 4002.240 (2001); Ill. Admin. Reg. Title 50 §§ 4001.10 to 4001.50 (2000); Ind. Admin. Title 760 R. 1 67 1 to 1 67 20 (2001); Iowa Admin. Code §§ 191 90.1 to 191 90.26 (2001/2002); Kan. Admin. Regs. § 40 1 46 (2001/2002); Kan. Stat. Ann. § 40 2404 (1955/2001); 806 Ky. Admin. Regs. 3:210 to 3:220 (2001/2002); La. Admin. Code 37:XIII.9901 to 37:XIII.9953 (Regulation 76) (2001); Me. Rev. Stat. Ann. Title 24 A § 2220 (2001); Mich. Comp. Laws §§ 500.501 to 500.547 (2001); Miss. Ins. Reg. 2000 1 (2001); Miss. Code Ann. § 83 1 45 (2001); Mo. Admin. Code Title 20 § 100 6.100 (2002); Mo. Rev. Stat. 362.422 (2001); Neb. Rev. Stat. § 44 901 to 44 925 (2001); Nev. Admin. Code (Uncodified) LCB File R130 01 (2002); Nev. Rev. Stat. § 686A.025 (2001); N.H. Admin. Code Ins. §§ 3001.01 to 3006.05 (2001); 13 N.M. Admin. Code §§ 13.1.3.1 to 13.1.3.29 (2002); N.M. Stat. Ann. § 59A 2 9.3 (2001); N.Y. Admin. Code Title 11 §§ 420.0 to 420.24 (Reg. 169) (2001); N.D. Admin. Code §§ 45 14 01 01 to 45 14 01 25 (2001); N.D. Cent. Code § 26.1 02 27 (2001); Okla. Ins. Regs. §§ 365:30 1 1 to 365:30 1 54 (2002); Okla. Stat. Title 36 § 307.2 (2001); OR. Admin. R. 836 080 0501 to 836 080 0551 (2002); Pa. Admin. Code Title 31 §§ 146a.1 to 146a 44 (2001); R.I. Regs. R27 99 001 to R27 99 021 (2001) (Financial); R27 100 001 to R27 100 013 (2001) (Health); S.C. Ins. R. 69 58 (2001); S.D. Admin. R. § 20:06:45 (2001); S.D. Codified Laws Ann. § 58 2 41 (2001); Tenn. Admin. Comp. ch. 0780 1 72 (2001); Tenn. Code Ann. § 56 8 119 (2001); 28 Tex. Admin. Code §§ 22.1to 22.26 (2001); 22.51 to 22.67 (2002); Tex. Ins. Code Ann. art. 28A.1 to 28A.102; 28B.01 to 28B.12 (2001); Utah Ins. R590 206 1 to 590 206 26 (2000/2002); Utah Code Ann. § 31A 23 317 (2001); VT. Admin. Comp. Ins. Dept. R. H 01 1 (2001); Wash. Admin. Code R. §§ 284 04 120 to 284 04 620 (2002); W. Va. Regs. §§ 114 57 1 to 144 57 22 (2001/2002) W.Va. Code § 33 6f 1 (2001); Wis. Admin. Code § Ins. 25.01 to 25.95 (2001/2002); Wyo. Ins. Regs. ch. 54 (2001); Wyo. Stat. § 26 2 133 (2001).

26. *NAIC's Priv. of Cons. Fin. and Health Info. Reg.* No. 672-1 § 4I, J (NAIC 2000). Specifically, section 4F(1) defines consumer as one who "seeks to obtain ... or has obtained an insurance product or service." (Emphasis added.) This definition expands the GLB Act definition of insurance consumers who are "customers" of a financial institution who obtain financial products or services for "personal, family or household purposes." 15 U.S.C. § 6809(9), (11). The GLB Act requires a privacy notice only "[a]t the time of establishing a customer relationship with a consumer" followed by an annual notice thereafter. 15 U.S.C. § 6803(a).

27. *NAIC's Priv. of Cons. Fin. and Health Info. Reg.* No. 672-1 § 4F(2)(d)(ii) (NAIC 2000).

28. *Id.* at §§ 17-22.

29. *Id.* at §§ 2A.

30. *Id.*

2. Health Insurance Portability And Accountability Act (HIPAA)

Another act that has wreaked havoc on the insurance, medical, internet technology and numerous other industries is the Health Insurance Portability and Accountability Act (HIPAA). The aim of this act is to limit use and release of private health information without the patient's consent.[31] It provides patients with the right of access to their medical records and to know if anyone else has accessed them. In November 1999, the U.S. Department of Health and Human Services (HHS) published the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule")[32] which modified the requirements in four significant areas: 1) eliminated the requirement for patient consent, 2) modified the definition of "marketing," 3) provided "incidental uses and disclosures" of protected information, and 4) provided additional time for compliance with the business associate provisions.[33] Civil and criminal sanctions are available for violations of the standards imposed.[34]

Who must comply with these standards? What types of insurance are not covered under HIPAA?[35] Although varied interpretations of this act and its regulations abound, it should be limited to health plans, health clearing houses, and health care providers who conduct certain financial and administrative transactions electronically, even if they contract other "business associates" to perform some of their essential functions. This law is not intended to provide authority to the HHS to regulate other private businesses such as employers, life insurance companies, workers compensation carriers, automobile medical payment carriers, automobile or general liability carriers, accident or disability income carriers, credit-only insurance, or public agencies that deliver social security or welfare benefits.[36] Although the HIPAA Privacy Rule only regulates covered entities and not business associates who transact business for a covered entity, the covered entity must provide ample protection in the business associate contract for the rights of access, amendment and accounting with respect to individuals' rights.[37]

3. Electronic Communications Privacy Act

Formerly known as the Federal Wiretapping Act, this act allows an employer to monitor employee e-mails as long as such monitoring is business related.[38] Stored messages must be protected from disclosure absent a search warrant (except as to the system operator) but cannot be divulged to others.[39] The penalties for violation estab-

31. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Pub. L. No. 104 191, 110 Stat. 1936 (1996). As early as 1976, the U.S. Supreme Court recognized privacy concerns created by the existence of large databases, saying, "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive governmental files." Whalen v. Roe, 429 U.S. 589, 605 (1976).

32. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918-60,065 (Nov. 3, 1999).

33. 45 C.F.R. §§ 160-164 (2002).

34. The standards are outlined in 45 C.F.R. § 160.306, 308. The civil penalties are $100.00 per violation up to $25,000.00 for multiple violations per year. The criminal penalties are up to $250,000.00 and ten years in prison.

35. http://answers.hhs.gov/cgi-bin.

36. 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). *See* 45 C.F.R. 160.103.

37. 45 C.F.R. 164.524, .526, and .528.

38. 18 U.S.C. §§ 2510-2522. Conversely, employers also risk liability by failing to monitor e-mails sent by employees. In Knox v. Indiana, 93 F.3d 1327 (7th Cir. 1996) a suit brought by a female corrections officer survived dismissal, summary judgment and was allowed to go to trial based in part on e mails the plaintiff had received from her supervisor asking her for sex. Furthermore, mere removal from an e-mail mailing list may be sufficient to state a cause of action against an employer by an employee. Hunt v. Rapides Healthcare Sys., LLC, 277 F.3d 757, 769 (5th Cir.)

39. However, numerous courts have held that the acquisition of stored electronic data, including e-mails, pager messages and even voice mail, does not violate the elements of 18 U.S.C. § 2510 regarding "interception" of electronic communications because the messages are no longer in the process of being transferred. *See, e.g.*, United States v. Reyes, 922 F. Supp. 818, 836 37 (S.D.N.Y. 1996) (citing United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (retrieving numbers stored in a pager's memory did not constitute interception of electronic communications); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D.Nev. 1996) (retrieval of alphanumeric pager messages stored in computer files did not constitute interception of electronic communications); United States v. Moriarty, 962 F. Supp. 217, 220 (D.Mass. 1997) (listening to stored voice mail messages is not interception because that form of access does not take place while information is in transmission); Wesley Coll. v. Pitts, 974 F. Supp. 375, 387 (D.Del. 1997) ("the plain language of the ECPA [18 U.S.C. § 2510 et seq.] reflects [that] Congress did not intend for 'intercept' to apply to electronic communications in 'electronic storage'"). As a matter of first impression and relying partly on the "flight"

lish a private cause of action.[40] Also, where a lawsuit occurs, e-mails potentially relevant to the subject matter thereof may be disclosed.[41]

4. International Privacy Protection

The international community has also taken steps toward establishing greater privacy protections. While there is consensus that privacy protection is beneficial and desirable, many steps taken so far appear to be *inviting* litigation on this issue.

On July 12, 2002, the European Communities of European Parliament passed their Electronic Communications Directive or "E-Privacy Directive," which provides for the confidentiality of communications as a guaranteed matter of human rights and fundamental freedoms.[42] Currently, the most celebrated part of the directive is the anti-spam measures, which prohibit e-mail solicitations without prior approval of the recipient.[43] The directive also extends to computers, wireless transmission (including e-mails), cell phones, on-star, pagers, vehicle tracking data, names and numbers. It also protects data regarding the parties contacted during the communication, the duration of the call, and even includes the preferences of communication chosen.[44] The directive provided an October 31, 2003 deadline for businesses to provide policies to users and to prevent security breaches.[45]

5. Spam

Unsolicited commercial e-mail, or "spam," now comprises 41 percent of all Internet e mail.[46] It is one of the most universally hated aspects of the new technological advances we have seen over the last decade.[47] A study by Ferris Research, reported in January 2003, estimates the annual cost of spam to U.S. corporations alone at $8.9 billion.[48] Several pieces of proposed legislation addressing the spam problem have emerged. In 2003, in the House of Representatives, HR 122 was introduced to prohibit use of the text, graphics or image messaging systems of wireless telephone systems to transmit unsolicited messages.[49] The proposed E-Mail Act of 2001, prohibited all unsolicited communication. The act allowed for an opt-out provision to be provided at the senders' website.[50]

Spam also has potential impact on wire-

---

requirements of interceptions, the Eleventh Circuit did not find a basis to suppress unlawfully intercepted electronic communications in the conviction of a child molester whose identity had been given to law enforcement by an anonymous computer "hacker" who gained access to the defendant's computer through the use of a virus or "trojan horse." U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003); *see* notes 72-74 below with accompanying discussion.

40. Damages are available to include the greater of "any profits the violator made as a result of the violation" or statutory damages of either $100.00 per day or $10,000.00, plus reasonable fees and costs. 18 U.S.C. § 2520.

41. However, 18 U.S.C. § 2517 does not authorize pretrial disclosure of wiretap evidence to private civil litigants. Nat'l. Broadcasting Co. v. U.S. Dept. of Justice, 735 F.2d 51 (2d Cir. 1984).

42. Council Directive 2002/58/EC of 12 July 2002, *Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, 2002 O.J. (L 201) 37. The new Directive particularly concerns itself with: 1) ensuring that individuals' rights and freedoms are protected with regard "to the increasing capacity for automated storage and processing of data relating to subscribers and users" of electronic communications services and 2) "minimizing the processing of personal data and of using anonymous or pseudonymous data where possible". Id. at Recital 7 and 9.

43. Britain and Italy have swiftly enacted legislation based upon the Directive imposing strict penalties. Under the new British law, violators face a fine of $8,057.00 if convicted by a magistrate judge. However, a fine from a jury trial is *unlimited*. The Italian law imposes a fine up to $101,600.00 and imposes a maximum prison term of three years.

44. C.D. 2002/58/EC, at Recital 15.

45. C.D. 2002/58/EC, Art. 17.

46. John B. Kennedy and Trey Hatch, *Recent Developments in Consumer Privacy: Focus on Spam and Identity Theft*, Practicing Law Institute PLI Order No. G0 01A2, Fourth Annual Institute on Privacy Law 2003: Protecting Your Client in a Security Conscious World (June, 2003).

47. The problem is truly a global one, as the international community continues to adopt anti-spamming measures. By October 31, 2003 the following twenty-six (26) countries were scheduled to forbid spam, without prior consent, by either fax or e-mail: Argentina, Australia, Austria, Belgium, Brazil, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, India, Ireland, Italy, Japan, Luxenburg, Netherlands, Norway, Portugal, Russia, South Korea, Spain, Sweden, the United Kingdom and Yugoslavia.

48. John B. Kennedy and Trey Hatch, *Recent Developments in Consumer Privacy: Focus on Spam and Identity Theft*, Practicing Law Institute PLI Order No. G0 01A2, Fourth Annual Institute on Privacy Law 2003: Protecting Your Client in a Security Conscious World (June, 2003).

49. The "Wireless Telephone Spam Protection Act" (HR 122) was introduced in January 2003 by Rush Holt (D NJ).

50. Incoming Senate Commerce Communications Subcommittee Chairman, Conrad Burns (R MT), named spam a centerpiece of his agenda. Burns sponsored the CAN SPAM Act, which was placed on the Senate Calendar for a vote in October 2002, but a vote never occurred.

less telephone communications. The Anti-Spamming Act was concerned with protection of children from unsolicited e-mails. Without federal protections against spam, states have been left to adopt their own measures of protection. Although numerous states (27) have adopted SPAM legislation. (Unfortunately for this writer, Florida is not among them.)

Disappointingly to some, recent interpretations of these statutes reveal that they do not have the "teeth" many would like. California courts have addressed the issue of e-mail solicitations under protection provided by state statute. In *Ferguson v. Friendfinders*,[51] the court considered e-mails that were deceptively misleading, in a purported attempt to be declared "non-advertisement." At issue was the application of section 17538.4, California Statutes, which prohibits e-mail advertisements. Although the e-mail in that case did not state it was an advertisement, no opt-out provisions were provided therein and the e-mail headers were altered to mask the identity of the sender. The action was based on negligence per se, trespass, unfair business practices and unlawful advertisement protection. The trial court dismissed the action. On appeal, although the California Fourth District Court of Appeal held the state statute constitutional, it upheld the dismissal, reasoning that no independent duty was mandated by the statute sufficient to create a private cause of action.[52]

Similarly, in *Aronson v. Brite Teeth*,[53] a Pennsylvania court held that no privacy protections against spam received via e-mail exist. In that case, the court held that spam protections were only applicable to faxes. Because the recipient did not have to read or print the e-mail, tie up the phone line until it was received, or waste ink or paper to print it, it was not sufficiently burdensome to require protection.[54] Going even further, a Missouri court actually struck down its state's anti-spamming law as an unconstitutional violation of advertisers' first amendment freedoms. *Missouri ex rel v. American Blast Fax*.[55]

In response to the divergent approaches by different states and courts, on June 11, 2003, a bill entitled "Stop Pornography and Abusive Marketing Act" or the "SPAM Act" was introduced into the Senate.[56] The SPAM Act is intended to eliminate the burdens and costs associated with spam by specifically targeting "unsolicited commercial electronic mail (UCE)."[57] In many ways similar to the March 11, 2003, Do Not Call Implementation Act[58] which created the widely publicized "National Do-Not Call Registry" (DNCR), discussed below, the Spam Act calls for the creation of a National No-Spam Registry by the Federal Trade Commission.[59] The SPAM Act does not contain a provision for criminal penalties, but provides for a $5,000.00 fine for each UCE sent to an e-mail address listed on the national No-Spam Registry[60] and imposes a maximum fine of $100,000.00 for each unauthorized use of the registry.[61] However, the SPAM Act does not actually prohibit spam, but instead requires all advertisements to contain "clear and conspicuous identification ... by providing, as the first characters in the subject line, 'ADV:'"[62] By inclusion of such information in the subject line, all advertisement e-mails could be easily screened by the recipient's e-mail program and deleted automatically. By imposing only content requirements, the SPAM Act does not appear to be subject to the same constitutional challenges as the DNCR, which actually prohibits telemarketing calls as discussed below.[63] However,

51. 94 Cal. App. 4th 1255 (Cal. App. 1st 2002)
52. *Id.*
53. 57 Pa. D & C 4th 1 (Pa. Com. Pl. 2002)
54. *Id.*
55. 196 F. Supp 2d 920 (E.D. Mo. 2002).
56. Introduced by Senator Charles Schumer of New York, the bill was referred to the Committee on Commerce, Science and Transportation on June 11, 2003. The bill was co-sponsored by Senators Graham (South Carolina) and Feingold (Wisconsin).
57. S.1231, s. 2(1).
58. Do Not Call Implementation Act, Pub. L. No. 108 10, 117 Stat. 557 (2003), codified at 15 U.S.C. §§ 6101 6108 (2003).
59. S.1231, s. 101.
60. S.1231, s. 102(b)(1).
61. S.1231, s. 102(b)(2).
62. S.1231, s. 201(a).
63. *See*, F.T.C. v. Mainstream Marketing Services, Inc., - F.3d - , 2003 WL 22293798 (10th Cir. 2003) and Mainstream Marketing Services, Inc. v. F.T.C., --- F. Supp. 2d , 2003 WL 22213517, 15 (D. Colo. 2003), at notes 76 and 77 below with corresponding discussion.

a positive ruling as to the constitutionality of the DNCR, may likely increase momentum and facilitate passage of the SPAM Act.

6. California SB 1386

One concern is that our pursuits for privacy protections may have unintended consequences and costs that threaten to outweigh the benefits of such protections. One recent example of this occurred in California, a state which is a typical forerunner on many issues that other states tend to follow. Therefore, a discussion of California's recent legislation is warranted.

In California, SB 1386 passed on September 25, 2002 (effective July 1, 2003) to regulate the dissemination of personal information by state agencies and businesses, and to ensure an accurate accounting of all disclosures.[64] The act provides for a strict retention period and requires all businesses to destroy all personal information when the business can no longer retain it. However, the act does not define "personal information" and the statutory retention period is mandatory. The act requires businesses that own or license computer data to notify California residents if personal information is disseminated as a result of a security breach.[65] The stated goal of the act is to prevent or reduce identity theft delay notification, providing only one exception: where informing the individual would impede a criminal investigation.[66]

The act also provides civil causes of action. However, questions exist regarding the appropriate statute of limitations applicable under the act. For example, if the cause of action is assumed to be based in contract, then the privacy policy could be interpreted to create a promise. The result is a blurred distinction between an intentional sale of data and a negligent dissemination of data. The potential for litigation as a result of this legislation is enormous.

7. USA PATRIOT Act

The USA PATRIOT Act is an acronym for Uniting and Strengthening America (U.S.A.) by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (P.A.T.R.I.O.T.). It probably took longer to come up with the acronym than it did to write the entire bill. After September 11, it seemed everyone was in favor of the act based on the title alone. It was enacted and signed by President George W. Bush on October 26, 2001.

The stated purpose of the act was to strengthen the country by creating an ability to combat terrorism and prevent money laundering (allegedly to terrorist groups).[67] Normally, race, ethnicity, religious beliefs and financial information are considered private. However, the act requires all financial institutions (of which insurance companies are a part) to develop anti-money laundering programs and to adopt minimum standards regarding the identities of customers opening accounts and/or customers purchasing policies of insurance. The act requires financial institutions to develop customer verification and documentation procedures and to determine whether the customer appears on the government's lists of known or suspected terrorists.[68] Such information gathering raises obvious questions of racial and ethnic profiling.

These requirements were effective as of April 24, 2003. The act permits disclosure and access to the following types of information:

1. Interceptions of wire, oral and electronic data.
2. Grand jury testimony and argument (historically considered *sacro sanct*).
3. Criminal investigation information.
4. Surveillance without a warrant.[69]
5. Physical searches.
6. Voice mail messages.

64. Codified at Cal. Civ. Code s. 1798.29 and s. 1798.82 (2003).

65. Cal. Civ. Code s. 1798.29(a) and s. 1798.82(a) (2003).

66. Cal. Civ. Code s. 1798.29(c) and s. 1798.82(c) (2003).

67. USA PATRIOT Act of 2001, Pub.L. No. 107 56 § 302, 115 Stat. 272 (codified at 18 U.S.C. § 1993).

68. USA PATRIOT Act of 2001, Pub. L. No. 107 56 § 326, 115 Stat. 272 (codified as amended in 31 U.S.C. § 5318).

69. The act's broad powers have potential impact on a variety of other legislation. An initial concern was the expansion of the Foreign Intelligence Surveillance Act (FISA) as amended by the Patriot Act. The determination was that such amendment was, in fact, constitutional. *In Re Sealed Case* 310 F.3d 717, U.S. FlSA Ct. of Review.

7. Foreign intelligence.
8. Business Records.
9. Trap and Trace devices /pen registers.
10. Nationwide service of search warrants.

Under the Act, law enforcement agencies can force internet service providers to disclose the methods and sources of payments for services, session times and duration.[70] This includes all network addresses, stored e-mail addresses, and whom they visit. Such disclosures will not violate the GLB Act (discussed *supra*). The act provides limited immunity under section 2707 (g)(1), Title 18 United States Code.

The act also provides for civil penalties if privacy is violated. However, the action can be stayed if it would adversely affect an on-going investigation. If there is a reasonable belief that an emergency exists involving danger of death or serious physical injury, all information may be disclosed.

Several courts have interpreted and upheld the USA PATRIOT Act. In *Handschu v. Special Services Division*,[71] a New York court heard a class action suit claiming certain surveillance activities violated constitutionally protected rights to privacy. Although this same issue was settled in New York over three decades ago, the NYPD requested modification. The court noted that, "*No basis* is discernable for doubting ... that law enforcement's ability to detect and guard against future terrorist attacks depends in large part upon the ability to *collect*, share and analyze information."[72] The court further recognized the restrictions on the NYPD's ability to disseminate information and stated, "*It is difficult to imagine a state of affairs more outdated* by the events of September 11th or out of step with the *urgent needs* of our law enforcement agencies."[73] On August 6, 2003, the court ordered that departmental rules governing police surveillance of political groups be placed under the court's supervision.[74] The court based its decision requiring a "strengthening of the Judgment" because of the "operational ignorance on the part of the NYPD's highest officials with respect to an investigatory technique resonant with constitutional overtones."[75]

In *US v. Steiger*, the Eleventh Circuit, considering an Alabama case, determined that the Patriot Act amended the Wiretap Act to only provide protection while communication is "in progress."[76] In that case, the defendant was convicted based upon tips provided to law enforcement from an anonymous computer "hacker" who gained access to the defendant's computer through the use of a virus. The Eleventh Circuit found no basis to suppress what it determined to be lawfully intercepted electronic communications.[77] Relying partly on the "flight" (active transmission) requirements of interceptions, the fact that the hacker obtained the information did not violate the Wiretap Act because the information gathered was "stored" rather than obtained during active transmission. The Court also specifically noted that Congress considered amending section 2515 in the USA Patriot Act to "extend the statutory exclusion rule in 18 U.S.C. § 2515 to electronic communications;" however, the Act was passed without such an amendment and therefore it must be construed to reflect that such provision was specifically rejected.[78]

In *Global Relief v. O'Neill*, *Powell, and Ashcroft*,[79] the court considered the case of Global Relief, an Islamic humanitarian relief organization whose assets were frozen subsequent to a search by the FBI. In denying Global Relief's preliminary injunction, the court reasoned that matters related to the conduct of foreign relations are so exclusively entrusted to the political branches to be largely immune from judi-

70. USA PATRIOT Act of 2001, Pub. L. No. 107 56 § 210, 115 Stat. 272 (codified as amended in 18 U.S.C. § 2703(d).
71. 273 F. Supp. 2d 327 (S.D.N.Y 2003).
72. *Id*. at 341.
73. *Id.*
74. --- F. Supp. 2d -, 2003 WL 21880456 (S.D.N.Y. 2003).
75. *Id.* at 6.
76. 318 F.3d 1039 (11th Cir. 2003).
77. *Id*. at 1050.
78. *Id.* at 1050, citing H.R.Rep. No. 236(I), at 8 (2001), with USA PATRIOT Act, Pub.L. No. 107 56, 115 Stat. 272 (2001).
79. 207 F. Supp. 2d 779 (N.D. Ill. 2002).

cial inquiry or interference. The holding demonstrates how "exceptionally strong"[80] the showing necessary to challenge the Executive Branch of government must be, even raising concerns over whether such a showing can ever be met.

8. Surveillance

Most corporations have the occasion to utilize surveillance techniques in their businesses, but it is not without a fear of litigation arising our of privacy violations. As noted above, the common law torts of negligent or intentional infliction of emotional distress for privacy violations are based on the four following elements: 1) unreasonable intrusion upon Plaintiff's seclusion; 2) public disclosure of private facts; 3) publicity which places one in a false light; and 4) violation of a privacy statute. Surveillance can create a cause of action for all four areas.

First, in considering whether an intrusion on seclusion occurred, a determination must be made whether the observations were contained in the private or public view. Second, surveillance on Plaintiff's property or viewing plaintiff inside his or her home may implicate a trespass. Third, publishing contents to state investigative agencies, insurance agents or co-workers with no claim handling responsibility or business need to receive such information may give rise to defamation claims. Fourth, surveillance conducted unreasonably may be a sufficient basis for a bad faith action. Fifth, talking with clients, customers, and/or business associates regarding the nature of a plaintiff or suggesting plaintiff burned down his own house, for example, can create a claim based on interference with business relationships.

A few courts have addressed the issue regarding legal liability for surveillance activities. For example, an Oregon court considered an action brought for trespass against an investigator who trespassed on Plaintiff's property to obtain film of the Plaintiff.[81] The court dismissed the Plaintiff's complaint because Plaintiff *did not know* the surveillance was on-going at the time. Conversely, an Alabama court determined that an investigation conducted from neighboring property, using high powered binoculars to film inside plaintiff's home *was unreasonable*.[82] In a particularly egregious case, a California court considered the case of a Plaintiff that was befriended by an investigator.[83] The investigator then took her to Disneyland while a co-investigator filmed them at the park. The court held the insurance company responsible for the lack of surveillance control.

Consequently, surveillance activities which are taken without regarding to the plaintiff's right to privacy can come back to adversely affect the entire claim which Plaintiff instituted in the first place.

9. National Do Not Call Registry (DNCR)

Finally, the creation of the National Do Not Call Registry (DNCR) is a tool which many hope to be substantially beneficial, but it is not without its litigation traps for the unwary. The DNCR is a national database administered by the Federal Trade Commission (FTC), with enforcement shared between the FTC and the Federal Communication Commission (FCC). In less than one week from the date of implementation, the FCC had received 2,379 complaints about alleged violations of the Do Not Call rules.[84] With such voluminous data and regulatory issues shared between two large federal agencies, questions of coordination and application are certain to arise. However, implementation by the separate agencies in consideration of other legislative issues - not to mention its constitu-

80. *Id.* at 788, quoting Palestine Info. Office v. Shultz, 674 F.Supp. 910, 918 (D.D.C.1987), aff'd, 853 F.2d 932 (1988) (citing Washington Metro. Area Transit Com'n v. Holiday Tours, Inc., 559 F.2d 841, 843 (D.C.Cir.1977)).

81. McLain v. Boise Cascade Corp., 533 P.2d 343 (Or. 1975).

82. Alabama Electric Cooperative, Inc. v. Partridge, 225 So. 2d 848 (Ala. 1969).

83. Unrah v. Truck Insurance Exchange, 498 P.2d 1063 (Cal. 1972).

84. FCC News Release, October 8, 2003 (the release also notes that during the same period the FCC logged 5,879 inquiries about the rules).

tionality - has already created questions of applicability to various industries.[85]

The development of the DNCR occurred on two separate plains, involving two separate pieces of legislation. The Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994, directed the FTC to "prescribe rules prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices.[86] The Act required that the rules provide "a definition of deceptive telemarketing acts or practices,"[87] and include "a requirement that telemarketers may not undertake a pattern of unsolicited telephone calls which the reasonable consumer would consider coercive or abusive of such consumer's right to privacy."[88] On January 29, 2003, the FTC issued the amended Telemarketing Sales Rule (TSR).[89] The 2003 amendment modified the original TSR,[90] by the inclusion of the highly publicized creation of the National DNCR.[91]

On March 11, 2003, the Do Not Call Implementation Act (Do Not Call Act) amending the Telemarketing and Consumer Fraud and Abuse Prevention Act was signed into law.[92] The Act also required the FCC to issue a final rule and to consult and coordinate with the FTC to maximize consistency with the FTC's 2002 amended TSR.[93] On July 3, 2003, the FCC released a Report and Order in CG Docket 02 278 revising the telemarketing rules and establishing the Do-Not-Call Registry with the FTC.[94]

The constitutional limitations of regulating commercial speech are articulated in *Central Hudson Gas & Elec. Corp. v. Public Service Commission*.[95] In *Central Hudson*, the Court considered the constitutionality of a New York Public Service Commission regulation that banned all advertisements by utilities. In striking down the regulation as unconstitutional, the Court identified a four-part test for determining whether restrictions on commercial speech are constitutional.[96] The first question is whether the speech in question concerns illegal activity or is misleading, in which case the government may freely regulate the speech. If the speech is not misleading and does not involve illegal activity, the court applies the rest of the four part test to the government's regulation. The second question is whether the government has a substantial interest in regulating the speech. Third, the government must show that the restriction on commercial speech directly and materially advances that interest. Finally, the regulation must be narrowly tailored to achieve that interest.

On September 25, 2003, the FTC rule was stricken as unconstitutional by a Federal District Court in Colorado.[97] Using the *Central Hudson* criteria, the District Court found the FTC rule unconstitutional because it granted certain exemptions, as the court saw it, based solely on content. Therefore, the court concluded that "[b]ecause the do not call registry distinguishes between the indistinct, it is unconstitutional under the First Amendment."[98] The Tenth Circuit Court of Appeals disagreed. Instead of applying the *Central Hudson* criteria independently, the court combined the final two criteria into a "reasonable fit" analysis, thereby staying the District Court's Order.[99] In so doing, the Court stated, "there is a substantial likelihood that the FTC will be able to show a

85. For example, the National Association of Independent Insurers' official position is that insurers are not required to comply with the National DNCR. Life Outlook: Clarification. Insurance Accounting, Vol. 14, No. 41 (October 20, 2003).

86. 15 U.S.C. § 6102(a)(1) (2003).

87. 15 U.S.C. § 6102(a)(2) (2003).

88. 15 U.S.C. § 6102(a)(3)(A) (2003).

89. The Telemarketing Sales Rule is codified in 15 U.S.C. §§ 6101 6108 (2003); the Rules and Regulations of the Federal Trade Commission are found at 16 CFR Part 310 (2003).

90. The FTC adopted the original Rule on August 16, 1995. 60 FR at 43842 (codified at 16 CFR 310 (1995)).

91. 16 CFR 310.4(b)(1)(iii)(B) (2003).

92. Do Not Call Implementation Act, Pub. L. No. 108 10, 117 Stat. 557 (2003), codified at 15 U.S.C. §§ 6101 6108 (2003).

93. Pub.L. 108 10, §3, 117 Stat. 557 (March 11, 2003).

94. Rules and Regulations Implementing the Telephone Consumer Protection Act (TCPA) of 1991, CG Docket No. 02 278, Report and Order, 68 FR 44144

95. 100 S. Ct. 2343 (1980).

96. *Id.* at 2351.

97. F.T.C. v. Mainstream Marketing Services, Inc., -F.3d-, 2003 WL 22293798 (10th Cir. 2003).

98. Mainstream Marketing Services, Inc. v. F.T.C., - F. Supp. 2d - , 2003 WL 22213517, 15 (D. Colo. 2003)

99. F.T.C. v. Mainstream Marketing Services, Inc., -F.3d-, 2003 WL 22293798, 2 (10th Cir. 2003).

reasonable fit between the substantial governmental interests it asserted and the national do not call list or, in other words, that the list directly advances the government's substantial interests and is narrowly tailored."[100]

Some in the insurance industry have argued that the Do Not Call rules do not apply to entities engaged in the business of insurance, not on First Amendment grounds, but because such rules conflict with the McCarran Ferguson Act (MFA) which provides that, "[t]he business of insurance ... shall be subject to the laws of the ... States which relate to the regulation ... of such business."[101] Additionally, the MFA provides that "[n]o Act of Congress shall be construed to invalidate, impair, or supersede any law enacted by any State for the purpose of regulating the business of insurance ... unless such Act specifically relates to the business of insurance."[102] The argument is that since insurers' marketing activities are extensively regulated at the state level, the Do-Not-Call rules "intrude upon the insurance regulatory framework established by the states and, therefore, should not be applicable to insurers under McCarran Ferguson."[103] Although such arguments have led some in the industry to take official positions that the current Do-Not-Call rules do not apply to insurance businesses, it remains an untested and unproven argument at this point.[104]

The FTC's position on the extension of the Do-Not-Call rules to the business of insurance is that the MFA provides that the FTC Act, and by extension, the TSR, are applicable to the business of insurance to the extent that such business is not regulated by state law. Whether the MFA exemption removes insurance related telemarketing from coverage of the TSR depends on the extent to which state law regulates the telemarketing at issue and whether enforcement of the TSR would conflict with, and effectively supersede, those state regulations.

The FTC was requested to clarify the exemption of registered broker dealers and insurance companies directly in the amended rule.[105] In response, the FTC stated that it was "unnecessary to exempt them by rule" because it "believes that the explicit statement of [its] jurisdictional limitation over broker dealers is abundantly clear in the Telemarketing Act itself."[106] Furthermore, the FTC's position on its jurisdiction is that the MFA's limitations are "clear, and thus no express exemption for [insurance businesses] is necessary."[107] Thus, unlike the jurisdictional exemptions for banks and non profit organizations, which do not extend to third party telemarketers making calls on their behalf, in the case of the telemarketing of insurance products and services, the TSR does not necessarily apply simply because the campaign is conducted by a third party telemarketer.

The FCC's jurisdictional position is similarly contingent upon the amount of state regulations of the individual insurance business. Although the FCC states explicitly that no additional authority is needed to regulate insurance under the new Do-Not-Call rules, it does so with a cautionary footnote.[108] The FCC clarifies that such an extension is based on their conclusion that the "McCarran Ferguson Act does not necessarily prohibit the application of the national registry to insurance companies."[109] Instead, the FCC determinations will be made given "the implications of the McCarran Ferguson Act [and] will need to be evaluated on a case by case basis."[110]

100. *Id.* at 9.

101. 15 U.S.C. § 1012(a) (2002).

102. 15 U.S.C. § 1012(b) (2002).

103. Comments of the American Council of Life Insurers (ACLI) as quoted in FCC Report and Order, 03-153, 33 (July 3, 2003).

104. Life Outlook: Clarification, Insurance Accounting, Vol. 14, No. 41 (October 20, 2003).

105. Citigroup and NAIFA comments as referenced by 16 CFR 310, Fed. Reg. Vol. 68, No. 19, 4587 (Jan. 29 2003).

106. *Id.*, citing 15 U.S.C. 6102(d)(2) (2002).

107. *Id.*, citing 15 U.S.C. 1012(b) of the McCarran Ferguson Act, for the proposition that "the business of insurance, to the extent that it is regulated by state law, is exempt from the Commission's jurisdiction pursuant to the FTC Act."

108. FCC Report and Order, 03-153, 29, note 152 (July 3, 2003).

109. *Id.*

110. *Id.*

III. Protections Against These Traps

No business decision is without risk. By making use of state of the art security models and technologies, companies have been able to reduce costs, improve the quality of products and services, and increase profits. Even after all cost-effective safeguards are in place, however, security and privacy risks still remain and cannot be reduced to zero, based upon the current state of technology, people and processes controls. The organization must continue its business notwithstanding the remaining risks.

The risks associated with security and privacy are increasingly a boardroom issue and certainly can impact operations, assets, financials, and brand equity. All that being said, technology and operations are certainly an important aspect of Sarbanes-Oxley, as IT underlies financial processes and the reliability of financial statements. Also security and privacy risks can represent an unforeseen, major impact on financials (if risk transfer through insurance is not part of a risk management program). For example, the current Directors & Officers Liability policies contain a "failure to maintain insurance" exclusion which could be invoked if senior management neither purchases or maintains adequate insurance to address its security and privacy risks.

Traditionally, contracts and insurance provide a means by which an organization can shift significant residual risk to a third party. With regard to contracts provided by technology and outside vendors, there is little to no risk transfer for consequential and liquidated damages. The contracts simply state that the vendor will make reasonable efforts to provide secure services, but without a transfer of risk. Therefore, a serious need exists for new insurance requirements and protections. Some of the protections, and their limitations, are discussed below:

Traditional insurance - commercial property, general liability, professional liability and crime insurance - will not provide the necessary coverage required to addressed security and privacy risks in a networked world. Traditional insurance was written for a world that no longer exists. Attempting to fit cyber risks into traditional insurance is like putting a square peg into a round hole. The key issues with traditional insurance are as follows:

- Elimination of computer virus coverage at meaningful limits from commercial property policies;
- Non-Physical Business Interruption (such as denial of service attacks) are not considered a direct physical loss;
- Contingent Risks (from external hosting, etc.) are not addressed by current policies;
- Crime policies require intent and do not cover stealing information (scope of coverage is money, security and tangible property);
- Data is not "tangible property" under a Commercial General Liability policy (which has been upheld in most court decisions)[111]. Therefore, theft or disclosure of third party information is not covered; and,
- Intentional acts exclusions in errors and omissions policies and the "occurrence" definition would remove coverage for the majority of security incidents, as inside perpetrators are frequently involved in these incidents.

Since 2000, a few insurers have introduced "cyber risks" insurance products to address security and privacy risks associated with network and Internet technologies. The majority market share of network security liability insurance is provided by AIG through its eBusiness Risk Solutions Division.[112] Other insurers include Lloyds of London and Zurich. The policies offered are non-admitted, and there are significant differences in policy terms and conditions between carriers. Be aware that insurance policies do not cover all possible losses and liabilities that an organization may sustain. The deductible or "outside the policy

111. *See* America Online, Inc. v. St. Paul Mercury Ins. Co., Civ. Action No. 01-1636-A (E.D. Va. Jun. 20, 2002) (insurer had no duty to defend under comprehensive general liability insurance policy covering "property damage" because software, data, and systems are not "tangible property").

112. Forbes; Business Week

scope" is the risk the organization assumes.

The coverage offerings available include:

Web Content Liability: Covers media offenses, intellectual property infringement (copyright, trademark, service mark) and invasion of privacy arising from the display of media on a web site. Patent infringement is specifically excluded.

Internet Technology Professional Liability: Covers technology professional services of Internet focused companies, such as application service providers, internet service providers, e-commerce transaction services, PKI services, managed security services, internet media services, hosting services, internet auction services, etc.
Network Security Liability: Covers legal liability and legal costs for claims arising out of computer attacks caused by failures of security including theft of client information, identity theft, negligent transmission of computer viruses and denial of service liability. Cyber-terrorism coverage options are available (as required under TRIA or broad form terrorism).

Data/Electronic Information Loss: Covers the cost of recollecting or retrieving first party data destroyed, damaged or corrupted due to a computer attack.

Business Interruption or Network Failure Expenses: Covers cost of lost net revenue and extra expense arising from a virus or denial of service attack. Especially valuable for computer networks with high availability needs.

Cyber-extortion: Covers both the cost of investigation and the extortion demand amount related to a threat to commit an intentional computer attack, implant a virus, etc.

As part of a sound risk management program for security and privacy risks, it is important for risk managers and General Counsel to review their insurance requirements for vendors, particularly vendors who provide technology services or who have sensitive network access/access to sensitive third party data. Liability will fall on the owner of the web site or the computer network, but it is important to make sure vendors have coverage to address their security breaches that impact your customers or other third parties. This is particularly important in industries that collect financial or health-related information of consumers. The discussion above concerning traditional insurance should prompt a review of insurance required of vendors and business partners. An example of a preferred security-focused insurance requirement in a vendor contract is as follows:

> Internet Liability Insurance including, without limitation, unauthorized access, unauthorized use, virus transmission, denial of service, personal injury, advertising injury, failure to protect privacy; and Intellectual Property Infringement covering the liability of the Vendor and the liability of [Company xxx] and its Affiliates arising out of the design, development, and/or maintenance of the systems used to operate and maintain the Services; with a minimum limit of not less than $5,000,000 per occurrence.

IV. Conclusion

As noted above, privacy and security interests remain a valued commodity internationally as well as for U.S. citizens. As privacy and security issues necessarily develop among individuals and business entities, the solutions offered in the form of regulations and statutory efforts are continuing to expand. Each adjustment in this area creates further rights and liabilities to all involved. Understanding the current atmosphere surrounding privacy and security legislation and potential violations of such is the first step towards protecting your business. Adding the appropriate risk transfers will instill even more confidence that your business is protected.

The Privacy Project II

How Good is Your Confidential Settlement Agreement?

Why defendants now need to be wary of how and where they enter into sealed settlement agreements and how they enforce them.[1]

By William B. Crow

Although often criticized for privatizing justice, sealed settlement agreements are useful tools in resolving disputes outside of court, and, if entered into without the court's assistance, should never become public record. During the past ten years, however, there has been an increasing trend granting the public access to court records, even those the parties intend to be confidential. This is especially true of documents that contain information related to what some would characterize as a disclosure of "public hazards," thus placing the public interest above the litigants' right to privacy. Fueled by media sensationalism and backed by the plaintiffs' bar, this latest trend has been marked by the enactment of many so-called "sunshine" acts. These acts create a more critical approach to granting sealing orders and require a balancing of the litigants' interests in confidentiality against the public interest in disclosure. The majority of the laws currently in force only restrict the sealing of settlement agreements entered into with the courts' assistance. Therefore, parties may still privately agree to seal settlement agreements out of court and incidentally prevent their agreement from coming within the provisions of most, but not all, of these sunshine acts. However parties, defendants especially, still need to be aware that should they ask the court to enforce their privately sealed settlement agreement it could become public record.

This article examines various state statutes, court rules and circuit case law that restricts the courts' ability to seal settlements. It also argues that courts and legislatures should not expand the acts to apply to agreements sealed without court involvement, even those agreements that might contain information relating to so-called public hazards.

Before discussing why privately sealed settlements should remain confidential and not be subject to disclosure, let us first examine why parties typically seek to seal settlement agreements.

Proponents of the public's right of access often bolster their argument against sealed settlements by claiming that sealed settlements are used primarily to hide important information from the public,[2] but in making that argument these proponents overlook the many valid reasons why defendants may seek confidentiality. Defendants often seek to seal settlement agreements to avoid becoming a "target defendant."[3] If settlement amounts are

IADC member William B. Crow joined Schwabe, Williamson & Wyatt in Portland as a shareholder of the firm in 2003, adding his internationally-recognized expertise to expand one of the most elite product liability practices in the nation. His trial and arbitration experience includes antitrust litigation, a variety of commercial disputes, securities claims, products liablity litigation, and insurance coverage issues. For the past ten years, Mr. Crow's peers have selected him as one of The Best Lawyers in America. In 2000, he was named one of Oregon's ten best litigators by the National Law Journal.

1. The author would like to give credit to Kathleen Blaner for her article *The Emperor Has No Clothes: How Courts Deny Protection for Confidential Information*, 70 Def. Couns. J. 12 (Jan. 2003) hereinafter Blaner. The author would also like to give credit and a special thanks to Christiane Rauh, for her invaluable assistance.

2. Arthur Miller, *Private Lives or Public Access?*, 77 A.B.A.J. 65, 66 (Aug. 1991) hereinafter Miller.

3. Sharon L. Sobczak, *To Seal or Not to Seal? In Search of Standards*, 60 Def. Couns. J. 406, 411 (July 1993) hereinafter Sobczak.

released to the public, defendant corporations and companies may be inundated by similar lawsuits filed by similarly situated plaintiffs looking to settle for the same amount of money.[4] Likewise, defendants look to protect trade secrets and certain proprietary information about their companies from being released to the public.[5] The release of this type of information could allow defendants' competitors to gain an unfair advantage, thus diminishing the commercial value of the information and the security provided by sealing.[6]

Not often discussed is why plaintiffs agree to seal settlements. It certainly cannot be the case that plaintiffs settle only after being strong-armed by defendants, or that plaintiffs agree to seal a settlement as their only avenue for pecuniary gain.[7] Sealed settlements and protective orders provide plaintiffs with privacy as well.[8] Plaintiffs are protected from charities, investment advisors, and family members seeking money post settlement.[9] Additionally, plaintiffs that are parties to cases of a sensitive nature such as sexual harassment or employment related claims can avoid publicity regarding facts related to their personal lives, medical and employment histories.[10]

Although sealed settlements offer protection for both plaintiffs and defendants, there is an ongoing debate as to whether they should be allowed. Below are the arguments often raised in opposition to, and in favor of, sealed settlement agreements.

Arguments Against Sealing

At the heart of the anti-sealing movement is a belief that litigation serves an inherently public function,[11] such that the public should have unrestricted access to all documents related to it. Furthermore, when the public is denied the opportunity to see the judicial process in action, its ability to understand the process is diminished, making the judicial process appear secretive and "mysterious."[12]

There are fundamental flaws in both of these arguments. First, simply because a litigant files a claim in a public court it does not follow that that litigant should then have to give up his right to privacy in order to have a conflict resolved.[13] Second, as far as privately sealed settlements are concerned, those agreements are reached without the assistance of a judge in issuing a sealing order; thus, there is no longer a public matter present, but a private contract to settle. As with private contracts entered into between businesses, the public should not be allowed access to the details of privately sealed settlements; public resources were not used in reaching the agreement and the parties did not appear in a public forum to have a sealing order issued. Third, when a case is settled out of court, the public does not lose an opportunity to gain a greater understanding of the judicial process. Settlement agreements replace the process either in whole or part; thus, you cannot lose an opportunity that never presented itself. As Arthur Miller points out in his article *Private Lives or Public Access?*, "[t]here has never been any right of public access to the activities, discussion and papers of the parties outside of the court during discovery or settlement;"[14] therefore, the public loses nothing by being left out of the details of settlement agreements.

Additionally, the argument that settlements preclude the public from a learning opportunity largely overstates the general public's interest in litigation. The public may not have been aware that a claim was

4. *Id.*
5. Miller, *supra* note 2 at 68.
6. *Id.*
7. Often a plaintiff's agreement to silence is their biggest bargaining chip and many choose to use it to their economic advantage.
8. Martha Neil, *Confidential Settlements Scrutinized: Recent Events Bolster Proponents of Limiting Secret Case Resolutions*, 88 A.B.A.J. 20, 22 (July 2002) hereinafter Neil; Carrie Menkel Meadow, *Whose Dispute is it Anyway? A Philosophical and Democratic Defense of Settlement* (In Some Cases), 83 Geo. L.J. 2663, 2684 (1995) hereinafter Meadow.
9. Neil, *supra* note 8 at 22.
10. Meadow, *supra* note 8 at 2684.
11. Sobczak, *supra* note 3 at 407
12. *Id* (this is often noted as one of the reasons why the public has a distrust for the judicial system).
13. Miller, *supra* note 2 at 68.
14. *Id.* at 65.

ever filed. Aside from highly publicized criminal and civil trials, it is unlikely that the public remains apprised of the thousands of cases filed in our nation's courts on a daily basis.

Next, those against sealing orders, the media especially, like to argue that much of the information contained in sealed settlement agreements affects the public health and safety, making it necessary for the public to access such information.[15] But often the important information that the media claims is present in sealed agreements is not there at all. Take the well-known Xerox case for example.[16] Xerox had allegedly hidden, within a sealed settlement, information related to the contamination of a neighborhood by hazardous waste.[17] It became known later that the only information contained within the settlement agreement was medical records of the plaintiff.[18]

Finally, those against sealing often argue that discovery of cash settlement amounts is necessary to facilitate trial strategy and preparation.[19] While the broadly drafted discovery rules were created to aid dispute resolution, they certainly were not created to assist attorneys in filing copycat lawsuits with similar claim amounts against deep-pocket defendants.[20] The courts are split in their treatment of this issue.[21] But theTexas Court of Appeals, for example, has held that a litigant requesting discovery of a settlement amount must demonstrate some relevancy beyond simply utilizing the information as a "comparative bargaining tool."[22]

Arguments in Favor of Sealing

Those in favor of sealed settlements believe that litigation serves an inherently private function, to which the public should not be granted access unless the parties allow it.[23] Litigants should not be forced to check their right to privacy at the door simply because they filed a lawsuit.[24] Whether parties enter into a court-assisted sealed settlement or agree to seal their settlement out of court and later seek the court's assistance to enforce it, their right to privacy should remain the paramount concern.

In addition to maintaining litigants' rights to privacy, confidential settlement agreements promote the free exchange of information between the parties and aid the resolution of disputes.[25] They also provide relief to courts with crowded dockets.[26] If parties are forced to reveal sensitive information despite an agreement to keep the terms of the settlement confidential, they may be deterred from entering into a settlement agreement at all.[27] Courts ought not be overburdened with cases that could have been settled out of court had this sensitive information remained confidential.

More important than freeing up court dockets, however, is the integrity of the sealed agreement itself. If the parties agree, between themselves, to seal their agreement it is not the courts' place to intervene and decide that such an agreement shall not be honored. If the plaintiff is the master of his or her complaint then both the parties should be the masters of their decision to seal their settlement agreement. The courts should not engage in evaluating whether a sealed settlement should be opened. By doing so their dockets will only become overburdened by actions to unseal agreements, thus both diminishing the benefit that settling out of court originally provided and causing the parties to feel that they do not own or control their own dispute.

Finally, if information from sealed settlement agreements is released to the public, there is a distinct possibility that following such disclosure adverse publicity might taint future juries hearing cases related to

15. *Id.* at 66-67.
16. *Id.* at 67; Sobczak, supra note 3 at 412.
17. *Id.*
18. *Id.*
19. Christine M. Tomko, Student Author, *Can You Keep a Secret?: Discoverability and Admissibility of Confidential Settlement Amounts in Ohio*, 52 Case W. L. Rev. 833, 841 (2002) hereinafter Tomko.
20. Miller, *supra* note 2 at 68.
21. Compare Bennett v. LaPere, 112 F.R.D. 136, 141 (D.R.I. 1986) (accepting the trial preparation argument) with Baby Doe v. Methacton Sch. Dist., 164 F.R.D. 175, 176-177 (E.D. Pa. 1995) (rejecting the trial preparation argument).
22. Tomko, *supra* note 20 at 843; *see* Palo Duro Pipeline Co., Inc. v. Cochran, 785 S.W.2d 455, 457 (Tex. App. 1990).
23. Sobczak, *supra* note 3 at 407.
24. *Id.* at 411; Miller, *supra* note 2 at 68.
25. Neil, *supra* note 8 at 20.
26. *Id.*
27. Sobczak, *supra* note 3 at 411.

the same product, manufacturer or company.[28] This publicity would hinder the ability of certain companies to receive fair trials and damage their professional reputations in general.

The courts and legislatures are engaged in an ongoing debate between a litigant's right to privacy and the public's right to information, some siding with the public and deciding that greater restrictions need to be placed on the ability to obtain a sealed settlement. Below are some of the most notable statutes and court rules currently in effect that create some of these new restrictions.

Florida

Florida enacted its "Sunshine in Litigation Act" in 1990.[29] This statute makes it unlawful for a court to seal any information that has the effect of "concealing a public hazard or *any information* concerning a public hazard . . . ."[30] Public hazards are defined as "[any] instrumentality, including . . . any device, instrument, person, procedure, or product . . . or condition of a device, person, procedure, or product that has caused and is likely to cause injury."[31] The statute creates a special exception for trade secrets, however, stating that trade secrets are not, by definition, public hazards.[32] As applied, if a settlement agreement is found to contain information regarding a public hazard then the court will unseal that information only -- the entire agreement will not be disclosed in whole.[33]

Florida courts interpreted this statute in 2000 and refused to unseal a private settlement agreement, holding that economic fraud in the leasing of vehicles was not a public hazard.[34] Florida case law has continually held that financial practices constituting economic fraud are not public hazards.[35] In comparison, Florida also refused to enforce a protective order issued by a federal district court at the joint request of all parties.[36] In *ACandS v. Askew*, 597 So. 2d 895, 896 (Fla. App. 1992), the respondent brought an asbestos action against ACandS in state court and wished to introduce information subject to the federally issued protective order.[37] The Florida Court of Appeals refused to enforce the protective order because some of the information protected related to a public hazard, asbestos.[38] ACandS argued that because the public was already well aware of the danger of asbestos, the protective order didn't violate Fla. Stat. § 69.081, but the court disagreed, stating that the statute prohibits a court order which conceals any information related to a public hazard.[39] By disallowing the sealing of documents that contain any information related to a hazard, it would seem that a party could merely allude to a hazard or product defect in its complaint and the court would refuse to grant a sealing, and/or, protective order. This is very troublesome and invades valid claims of a right to privacy.

Texas

Texas Rule of Civil Procedure 76a, similar to the Florida statute, applies only to court records containing information that could have an adverse effect on the health and safety of the public.[40] This rule operates to create a presumption that all court records are "open to the general public."[41] This presumption may be overcome only by a showing of a substantial interest that outweighs the presumption of openness and any adverse affect that sealing may have on the public.[42] Additionally, the party in favor

28. *Id.*
29. Fla. Stat. § 69.081
30. *Id.* § 69.081(3) (emphasis added).
31. *Id*. § 69.081(2).
32. *Id*. § 69.081(5).
33. *Id*. § 69.081(7).
34. *See* Stivers v. Ford Motor Credit Co., 2000 Fla. App. LEXIS 16980 (2000) (Ford sought to enforce the confidentiality agreement between itself and the appellant; appellant claimed the agreement was not enforceable under Fla. Stat. § 69.081; the court disagreed).
35. State Farm Fire and Casualty Co. v. Sonsnowski, 830 So. 2d 886, 887 (Fla. App. 2002).
36. ACandS, Inc. v. Askew, 597 So. 2d 895, 896 (Fla. App. 1992).
37. *Id*.
38. *Id.* at 896-897.
39. *Id*. at 898-899.
40. *See generally* Tex. R. Civ. Proc. 76a.
41. *Id*. at 76a(1).
42. *Id.* at 76a(1)(a).

of sealing must demonstrate that there is no less restrictive means of protecting the substantial interest asserted.[43] This rule makes exceptions for documents to which access is otherwise restricted by law, such as documents from adoption, juvenile, mental health, and family cases.[44] Moreover, reference to settlement amounts, or monetary consideration, is not defined as a "court record" subject to the presumption created under the rule.[45]

Those parties concerned only with the release of settlement amounts can breathe a sigh of relief because this rule would not restrict their ability to keep that information confidential. Parties sealing out of court settlement agreements may also be inclined to relax, but they should note that this rule is also applicable to settlement agreements "*not filed of record*."[46] Therefore, if a Texas court, asked to interpret or enforce a privately sealed settlement, found that the protected interests did not outweigh the public interest in disclosure, the agreement could become public knowledge. This radically affects the confidence with which parties may enter into a sealed settlement out of court, knowing that such a contract might later be undermined.

David Luban argues that this rule, and other sunshine acts, do not do away with protective orders, but merely shift the burden necessary to obtain a protective order to the requesting party.[47] But the burden of proof to overcome the presumption of openness in these cases is so great that describing it as a simple "shift" is to understate what these rules entail. Moreover, the Texas rule applies to settlements not filed with the court; this doesn't shift the burden of proof, but creates one. Luban also argues, in response to those alarmed by the implications of this rule, that it would be "farfetched" to assume that a person's medical history or condition, for example, could be considered public health and safety information.[48] He goes on to say that in the case of protecting someone's medical history or condition a judge would certainly invoke one of the exceptions to 76a and grant a sealing order.[49] But, the Texas Court of Appeals actually refused to overturn a lower court decision declining to grant a protective order despite the appellant's desire to keep confidential his medical condition.[50] The trial court judge in this case had found that this litigant's privacy interest was not an exception to the rule, and that it did not outweigh the public interest in disclosure. Luban's hypothetical is not so farfetched after all.

New York

New York will only allow courts to seal records, in whole or part, if the party in favor of sealing shows *good cause*.[51] Unfortunately, the rule does not define "good cause" other than to state that in determining its presence, the courts shall consider the public interest and the interests of the parties.[52] This rule does not apply, however, to discovery or protective orders,[53] nor does it apply to settlements filed out of court.[54]

The New York courts applied this rule in a 1992 case.[55] The court determined that good cause was demonstrated by a couple wishing to seal the records in their son's wrongful death case because the records contained no information relating to defective products or public safety.[56] Good cause was also shown in a case involving the abortion pill RU-486.[57] The court found

43. *Id* at 76a(1)(b) (redaction or sealing only certain documents for example)
44. *Id.* at 76a(2)(a)
45. *Id.* at 76a(2)(b) (including settlement agreements not filed of records in the definition of court records, but excluding references to monetary consideration).
46. *Id.*
47. David Luban, Settlements and the Erosion of the Public Realm, 83 Geo. L.J. 2619, 2654 (1995) hereinafter Luban.
48. *Id.*
49. *Id.*
50. D.B. v. Rodriguez, 2000 Tex. App. LEXIS 8120 (2000). N.Y. CLS Unif. R. Tr. Cts. § 216.1 (similar to the Texas rule whereby a substantial interest that outweighs the public interest must be shown).
51. *See id.*
52. Miller, *supra* note 2 at 66.
53. Luban, *supra* note 47.at n. 128.
54. *In re Estate of RR*, 53 Misc. 2d 747; N.Y.S.2d 644 (1992).
55. *See id.* (sealing allowed to guard against curiosity of third parties, etc.).
56. Danco Lab, Ltd. v. Chemical Works of Gedeon Richter, Ltd., 274 A.D.2d 1 (N.Y. App. Div. 2000)
57. *Id.* at 8.

good cause for keeping business information confidential as well as the names of parties involved in the case who could become subject to harassment if their names were revealed.[58] However, the court held that the appropriate remedy was not a total sealing order, as had been granted by the trial court, but to redact the protected information.[59]

South Carolina

The South Carolina federal district court has issued the strictest rule pertaining to sealed settlements, Local Civil Rule 5.03(c). In fact, no settlement agreements filed in the district courts are to be sealed, with no exceptions.[60] It should be reiterated that this is a federal district court rule; thus, the rule does not apply to settlements filed in South Carolina State courts.[61] Nor does the rule apply to settlements reached out of court.[62]

This rule is unambiguous and leaves little room for interpretation; there are no sealed settlements in this court. The rule does not apply to settlements reached out of court, but it doesn't designate how the courts are to treat out-of-court sealed settlements when the parties ask the court to enforce or interpret them.

These statutes and court rules give us some idea as to how certain jurisdictions might treat a request for a court issued sealed settlement agreement. However, they leave uncertainty as to how courts will treat requests to enforce, or unseal, sealed settlement agreements reached without court assistance, privately, by the parties to a controversy. But whatever uncertainties have been created, courts should not engage in the unsealing of private confidential settlement agreements. It is not the role of the courts to do so, they are not well equipped to decide when it is appropriate, and it undermines the integrity of this type of contract.

The Seventh Circuit has already held that when a party asks the court to interpret its confidential settlement agreement, the agreement becomes a public record. That court stated that the desire to avoid dissemination of a settlement amount is "not nearly on a par with national security and trade secret information."[63] Likewise, the Third Circuit has stated that "in some circumstances, a private agreement to keep terms of a settlement confidential may be unenforceable because it violates public policy."[64] Furthermore, the Texas rule, as discussed above, applies the presumption of openness to records not filed with the court, which most likely includes confidential settlement agreements reached outside of court.[65]

Assume, for the sake of argument, that it is the courts' job to preside over privately sealed documents and to unseal them if they contain information relating to a public hazard. What will be the standard by which the courts determine if a public hazard is present? What methodology will be employed to ensure that the courts are not unsealing documents based on naked allegations of hazardous products or defects with only scant evidentiary support? Will judges do more than draw an arbitrary line in the sand before declaring the presence of a public hazard?

It is not, and should not become, the courts' role to spend precious judicial resources determining when a sealed document should become public record simply because it makes mention of something affecting the public health and welfare. Courts already have a difficult time decid-

58. *Id.*

59. D.S.C. Local Civ. R. 5.03

60. Andrews Publications, S.C. Federal Court Bans Secrecy in Court Approved Settlements, 8 No. 6 Andrews Health Care Fraud Litig. Reptr. 6 (Jan. 2003).

61. *Id.*

62. Herrnreiter v. Chi. Hous. Auth., 281 F.3d 634, 636-637 (2002) (holding that an interest in non-disclosure of a settlement amount could not overcome presumption of openness, unlike the interest in protecting trade secrets).

63. Pansey v. Borough of Stroudsburg, 23 F.3d 772, 788 n. 21(3rd Cir. 1994).

64. *See* discussion at page 9 *infra*.

65. Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579, 113 S. Ct. 2786 (1993) (creating a new standard to judge the reliability of scientific evidence, including whether the theory in question can, and has, been tested, whether the theory has been the subject of peer review or publication, the known or potential rate of error associated with the method, the degree of acceptance in the relevant scientific community).

ing whether or not scientific evidence is credible and spend a great amount of time and money in deciding whether it should be admissible, even post *Daubert*.[66] Judges do not often hold technical or scientific degrees; thus, they are no better equipped than the average person to determine what reliable scientific evidence and methodology look like. It would seem that the same is true of their ability to spot a legitimate public hazard. As Sharon Sobczak put it, "even if judges had the scientific or medical expertise necessary to evaluate the data usually implicated when health and safety are at issue, they would be undertaking tasks not even remotely related to their primary function of deciding the cases before them and presiding over settled cases."[67]

Even if judges had the skills required to make decisions related to the public health and safety, the use of notice pleading might well make the allegations upon which these judges base their decisions to unseal settlements the deciding factor in unsealing a settlement agreement, thus making the allegations sufficient to avoid summary dismissal the criteria in questions of public hazard.[68] Arthur Miller argues that "although the allegations made in a complaint may raise issues that appear to implicate matters affecting public health and safety, and information produced in discovery may appear to confirm that, the truth of the allegations can be known only after they have been tested through the full litigation process."[69] To unseal information contained in a document, like a settlement agreement, that was created in place of a full trial could be as Miller says "premature . . . and destructive to a litigant's reputation or business . . . ."[70]

The Audi 5000 case is an example of the destructive effects that premature disclosure of information can have.[71] Before the case against Audi had been fully tried, the media disclosed preliminary information to the public that the Audi 5000 suffered from an acceleration defect that caused numerous accidents and deaths.[72] This information caused the public to cease buying the car and inflicted severe damage on Audi's reputation.[73] It was only after the media hype, and several trials, that it was revealed that a driver error, not an acceleration defect, was the cause of the accidents and deaths.[74] Audi would have benefited greatly from a sealing order, and the public would not have suffered. Likewise it is easy to see from this example the destructive result that would have been produced had Audi settled before trial and the court later unsealed the agreement. There would have been no trial to flush out the true cause of the accident and the erroneous preliminary information would have been disseminated to the public.

The media would have the public believe that sealed settlements always contain information related to public hazards and that public access is proper to protect the public welfare. While it may be the media's job to keep the public informed, it is not the media's job to step into the realm of the federal regulatory bodies and attempt to cure societal wrongs by gaining access to sealed information.[75] Nor is it the role of the courts to act as the arbiters charged with maintaining public safety, instead of the administrative agencies dedicated to that very purpose.[76] As Sobczak argues, these agencies have the power to "investigate, subpoena documents and demand answers."[77] Until sealed settlement agreements prevent these agencies from performing their job, then the information within sealed settlements should not be disseminated to the public.

In conclusion, despite the trend to restrict courts' ability to grant sealing/protective orders, many states have rejected similar legislation, including Arkansas,

66. Sobczak, *supra* note 3 at 412-413.
67. Discovery is where claimants typically gain the bulk of their evidentiary support.
68. Miller, *supra* note 2 at 67.
69. *Id.*
70. Blaner, *supra* note 1 at 14; Miller *supra* note 2 at 67; Sobczak, *supra* note 3 at 412.
71. Miller, *supra* note 2 at 67.; Sobczak, *supra* note 3 at 412.
72. *Id.*
73. *Id.*
74. Sobczak, *supra* note 3 at 412.
75. *Id.*
76. *Id.*
77. Miller, *supra* note 2 at 66.

Colorado, Hawaii, Idaho, Iowa, Kansas, Michigan, Montana, New Mexico, South Dakota, and Virginia.[78] In fact, very few states are even considering legislation to place restrictions on sealed settlements.[79] In light of this it seems unlikely that sealed settlements will cease to exist anytime soon. Likewise, it seems unlikely that the courts will unseal settlement agreements to satisfy the idle curiosity of third parties. But, as for their decisions when the requesting party presents more than idle curiosity as the reason for unsealing, the answer is less certain. The bottom line is that parties need to be aware that if they agree to seal their settlement in a state with an active sunshine act, they need to prepare themselves for the possibility that the information therein could become public record.

78. Neil, *supra* note 8 at 22.
79. Neil, *supra* note 8 at 22.

Expanding Tort Liability of Information Providers: How Far Can Forseability Be Stretched?

By Dennis T. Ducharme

IADC member Dennis T. Ducharme is a Partner and head of the Insurance Practice Group at Wiggin & Nourie, P.A. in Manchester, N.H. He is a member of the IADC Products Liability and Drug, Device and Biotechnology Committees. He is a 1982 graduate of The Massachusetts College of Liberal Arts (B.A., summa cum laude, 1982) and The Georgetown University Law Center (J.D., 1985).

A. Introduction

Technological advancements have created ever-expanding capacities for the collection and dissemination of private information. As the ability to collect and use such data has increased, so has its marketability. While general concerns about the erosion of privacy caused by such practices have been voiced by many, it has been suggested that the protection of privacy rights for the people about whom this information is gathered are lacking. Many scholars and privacy advocates have suggested that neither statutory nor common law remedies for those who believe their privacy rights have been invaded are adequate.

In one recent case, *Remsburg v. Docusearch Inc.*,[1] the New Hampshire Supreme Court acknowledged a cause of action against an internet information provider based solely on a foreseeability analysis. The Court did so without reliance on either a statutory remedy or any of the recognized "privacy" torts under the Restatement, (Second) of Torts. While some authors have hailed the *Remsburg* decision as a positive step in the protection of privacy rights, this article considers whether the New Hampshire Supreme Court may have gone too far in its decision; opening far too many parties who process private information to potential tort liability.

B. The Expansion of Information Gathering Technology

In 1890 Warren and Brandeis showed incredible foresight when they wrote a note which warned of "mechanical devices" which "threatened to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[2] Widely recognized as the seminal work in the development of "privacy law," the Warren and Brandeis note was concerned primarily with yellow journalism and the over zealousness of the press. While those particular concerns are as prevalent as ever, technology has played a significant role in creating an ever-expanding list of concerns about the erosion of privacy in our lives. Warren and Brandeis could not have conceivably foreseen the "mechanical devices" which dominate our lives just over 100 years later, much less the myriad uses of the information collected and stored by those devices or the volume of debate concerning their impact on privacy rights.

Day after day, we engage in transactions which leave an information trail behind us. While that information may not be "proclaimed from the house-tops," it is collected, sorted, sold and resold with mind numbing regularity. A trip to the grocery store where we use a preferred customer card adds our name, and the types of products

1. Remsburg v. Docusearch Inc., 816 A.2d 1001; 2003 N.H. Lexis 17 (February 18, 2003)

2. Warren and Brandeis, *The Right to Privacy*, 4 Har. L. Rev. 193, 195 (1890)

we buy to a database.[3] Use of an "easy pass" card on the highway tells those who control data where we were and when.[4] In many automobiles, we are the press of a button away from being tracked by the manufacturer who sold us the car. Records of the books we buy or check out at libraries are kept with greater and greater regularity. When we use the Internet, we leave an array of information behind which is tracked, collated, and then bought and sold time and time again.[5] Much of our biographical makeup is collected and collated without our knowledge, and then sold for a variety of purposes by those doing the collecting and collating.[6]

In addition to the many types of data collection of which we are vaguely aware, there are emerging technologies which create additional means by which our privacy could be invaded about which most of us are completely in the dark. "Locator chips" are being used with greater regularity. These chips are somewhat like the tracking devices we have seen James Bond use in movies over they years. One common use of such technology is the timing device used in large road races which allow officials to track the entire field with greater efficiency and accuracy. In addition, however, this same technology is being used to track product inventory in many settings.[7] Concerns have been raised about the potential misuse for such technology including the potential for consumers to be "tracked" in the interest of future market research data.[8] Another area where information is gathered about us without much awareness is airbag technology which is in place in many motor vehicles. Sensors installed in many cars record data such as speed and the status of other mechanical systems in cars in the last few seconds leading up to the deployment of an airbag. Emerging issues arising out of that technology include questions as to just who "owns" the information, how reliable the data is, and how it may be discovered and used during civil and criminal proceedings.[9]

While intrusions on our privacy resulting from generally benign data gathering are usually no more than a nuisance - we just do not like having the cash register clerk ask for our zip code or phone number; the data collected is frequently used in much more insidious ways. Michael Froomkin, author of *The Death Of Privacy?* takes an in depth look at the dark side of "data mining," a phenomenon that takes the collection of personal data to extremely intrusive and potentially harmful levels.[10] Froomkin discusses the ability of one to buy lists based on anything from broad categories such as ethnicity, political opinion or sexual orientation to narrow categories such as lists of college students sorted by major, children who have subscribed to a particular magazine, or those who purchase skimpy underwear, among others.[11] Parties collecting, collating, and selling data of this type are doing so not simply for the sake of doing so but because somebody wants the

3. At least one form of seemingly benign data, who buys small plastic bags and baking powder, became a lead for the DEA and the subject of press in a major newspaper. The DEA sought this information because those products are commonly the tools of drug dealers. *See* Berman and Mulligan, *Privacy In The Digital Age: Work in Progress*, 23 Nova L. Rev. 549 (1999) (Discussing Washington Post Article and DEA activity) It is easy to imagine any number of logical links between products and "suspicious" activity based on profiles which the DEA, FBI or other police agencies may develop.

4. In at least one jurisdiction, the State of Virginia, Department of Transportation officials have received discovery requests for such data, as of this date, primarily in the criminal context. *See Is Big Brother In The Tollbooth?* The Hampton Daily Press, November 14, 2002.

5. *See*, *e.g.* Berman and Mulligan, *supra* 23 Nova L. Rev. 549, 554 (1999) (Discussing Internet data trails and "digital fingerprints" left behind by use of the Internet)

6. For excellent overviews of the scope of information collected and their impact of biographical "aggregation," see generally, Daniel Solove, *Modern Studies In Privacy Law*; *Notice, Autonomy and Enforcement of Data Privacy Legislation*, 86 Minn. L. Rev. 1137 (2002); Will Thomas DeVries, *Annual Review Of Law And Technology: III. Protecting Privacy In The Digital Age* 18 Berkley Tech. L. J. 283 (2003)

7. Yue, Tags Pit Efficiency vs. Privacy, Chicago Tribune, July 15, 2003.

8. *Id.*

9. *See e.g.* David Uris, *Big Brother and a Little Black Box: The Effect of Scientific Evidence on Privacy Rights*, 42 Santa Clara L. Rev. 995 (2002); David M. Katz, *Privacy in the Private Sector: Use of the Automotive Industry's "Event Data Recorder" and Cable Industry's "Interactive Television" In Collecting Personal Data*, 29 Rutgers Computer & Tech. L. J. 163 (2003)

10. *See* A. Michael Froomkin, *Symposium: Cyberspace and Privacy; A New Legal Paradigm? The Death Of Privacy?* 52 Stan. L. Rev. 1461 (2000)

11. *Id.* at 1470, n.22.

data and is willing to pay for it.

While most of the buyers of data probably purchase it for relatively harmless purposes i.e. to try to sell us something, the risks of such data being used for more invasive and harmful purposes are obvious. This is particularly so when lists lend themselves to targeting by buyers motivated to harm members of an ethnic group or to have a "hit list," based on some other personal trait common to the people making up the list.

Significant public policy questions are presented as to just what rights and remedies we have as individuals about whom this data is being collected and then sold. To whom may we turn when we believe we have been harmed? What damages may we recover when we believe we have been harmed? One very important question is the extent to which modern tort law will be able to keep pace with the continuing expansion of this market place for information.[12]

C. "Privacy Law" as a Protection?

"Privacy law" as a substantive body of law has many divergent threads, all of which many commentators would suggest trace their roots in some fashion back to the Warren and Brandeis article.[13] With regard to torts, most agree that Dean Prosser's work, both his landmark article in 1960, and his work as the reporter for the second restatement, provides the foundation for virtually all-existing case law.[14]

The privacy torts include four distinct causes of action originally described by Dean Prosser and eventually codified in the restatement, second of torts. As Prosser described them, they included:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
2. Public disclosure of embarrassing private facts about the plaintiff;
3. Publicity which places the plaintiff in a false light in the public eye;
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[15]

The third and fourth privacy torts, now codified in the Restatement at sections 652 D and E have been, to a great extent, subsumed in to the substantive body of defamation law. Most claims for libel or slander will have parallel claims for either false light, misappropriation of the plaintiff's name or likeness, or both.[16] Claims for improper dissemination or use of collected biographical data lend themselves more readily to claims based on the first two torts identified by Dean Prosser and then codified in the Restatement at sections 652 B and C. As the collection and redissemination of facts about individuals becomes more and more prevalent, the risk of harm, or perceived harm from such dissemination has gone through a natural expansion.

Much as we are living in an age of information explosion, we are also living in an age marked by an explosion of commentary on privacy law issues. A number of commentators considering the potential remedies for either intrusion upon seclusion or the public disclosure of embarrassing facts share the parallel views that the courts have underutilized the restatement torts as a tool to protect privacy interests and that privacy law in its current state cannot keep pace with growing technological encroachments on people's privacy rights.[17]

The privacy torts have been criticized as not adequately protecting aggrieved parties in such situations. Andrew J. McClurg has argued that the courts have not favorably received claims based on the privacy torts and goes so far as to suggest that the harsh

12. A number of commentators have addressed the patchwork nature of statutory remedies available, recognizing the substantial number of remedial gaps resulting from the lack of a comprehensive statutory scheme. *See generally*, DeVries, *supra*, pp. 288 - 91; Solove, *Privacy And Power: Computer Databases And Metaphors For Information Privacy*, 53 Stan. L. Rev. 1393 (2001), 1440 - 44.

13. This article is not intended to be a comprehensive review of "privacy law." In particular, it does not address either statutory issues, or Constitutional based privacy theories.

14. *See generally*, Solove, *supra*, 53 Stan. L. Rev. 1393 (2001); Andrew J. McClurg, *Bringing Privacy Law Out Of The Closet: A Tort Theory Of Liability For Intrusions In Public Places*, 73 N.C.L. Rev. 989 (1995).

15. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960); *See generally*, Restatement (Second) of Torts 652B-652E (1977)

16. McClurg describes "false light" as the "sickly stepchild" of defamation.

17. *See generally*, DeVries, *supra*, Froomkin, *supra*.

treatment plaintiffs receive when making such claims bring into question whether or not a cause of action for invasion of privacy even exists.[18] He cites a host of statistics supporting his thesis, including an incredibly high percentage of cases being disposed of by summary judgment, preventing plaintiffs from even being allowed to present their cases to a jury.[19]

Daniel Solove is equally critical of the manner in which the courts have treated those alleging privacy torts, pointing out the inherent conflict in a tort which requires intrusion into private affairs as an element and thereby gives inadequate protection to parties harmed by disclosure of information which is in some way public.[20] Simply put, Solove articulates a compelling problem created by the fact that we live in a society where so much information about us is "public." Because a great deal of information which we used to consider to be private is now in the public domain, a tort requiring disclosure of private facts to sustain a cause of action allows those who collect and sell data to do so with increasing impunity. If the mere fact that a piece of data appears in some public record allows it to be used with no recourse, claims for public disclosure of private facts will almost never succeed.[21]

The expansion of technology and explosion of information collected and disseminated by that technology is exponential. In 1995 Andrew J. McClurg published an insightful article also opining that the Restatement torts had been underutilized by the courts as a tool to protect the right of privacy. At that time, he believed the greatest threat to privacy was the burgeoning use of the video camera to record individuals' activities in public places and advocated for a multifactor approach in redefining the tort of "intrusion" in public places.[22] In barely half a decade after that, scores of articles addressed the continuing erosion of privacy focusing on an even broader range of intrusions into privacy created by Internet transactions, cash register transactions, and the ever-expanding network of technologies which gather information about us and then disseminate that information, often for profit, and usually without our permission.[23]

While Warren and Brandeis wrote of our right to be "let alone"[24] and Brandeis later expounded on that theory from the bench[25] one could certainly argue that the notion of a right to be "let alone" is in many ways no more than an historical anomaly.[26] While a patchwork of legislation geared to protect privacy in specific subject areas has begun to emerge,[27] we still live in a society where more and more people are throwing up their

18. McClurg, *supra*.

19. *Id.* at 999 - 1003.

20. Solove, *supra*, at 1181-84.

21. If the mere fact that a piece of data appears in *some* public record allows it to be used with no recourse, claims for public disclosure of private facts will almost never succeed. A number of courts have rejected claims for public disclosure of private facts because the facts had some marginal and often quite stale, connection to the private domain. *See, e.g.*, Jenkins v. Bolla, 411 Pa. Super 119, 600 A.2d 1293 (Pa. 1992) (No privacy right in redisclosure of convictions as old as 35 years); Montesento v. Donrey Media Group, 99 Nev. 644, 668 P. 2d 1081 (Nev. 1983) (facts drawn from public records cannot form basis for claim for disclosure of embarrassing private facts).

22. McClurg, *supra*.

23. *See generally*, *e.g.*, Solove, *supra*, 86 Min. L. Rev. 1137; DeVries, *Annual Review Of Law And Technology: III. Protecting Privacy In The Digital Age* 18 Berkley Tech. L. J. 283 (2003); McClurg, *supra*, 73 N. C. L. Rev. 989; Solove, *Privacy And Power: Computer Databases And Metaphors For Information Privacy*, 53 Stan. L. Rev. 1393 (2001); Froomkin, *supra*, 52 Stan. L. Rev. 1461

24. Warren and Brandeis, *supra*, at 195, 205.

25. In Olmstead v. United States, 277 U.S. 438, 478 (1928), writing in the context of a decision concerning government action rather than private action, Brandeis discussed the framers' recognizition of " the right to be let alone" as being the right *most valued* by civilized men.

26. One particularly troubling decision in the manner in which it cites the Warren and Brandeis article is Bartnicki v. Vopper, 532 U. S. 514 (2001). In Bartnicki v. Vopper the United States Supreme Court considered the degree to which the First Amendment protected radio disc jockeys who repeatedly replayed a tape of an illegally intercepted cell phone call which they knew was illegally intercepted by an unknown third party. In finding that the First Amendment protected the redisclosure under the circumstances in question, in great part because the subject matter at issue, local teacher negotiations, was one of public interest, the Supreme Court quoted Warren and Brandeis for the proposition that "the right of privacy does not prohibit any publication of matter which is of public or general interest." *The Right To Privacy*, 4 Har. L. Rev. at 214. The quote utilized is a direct quote of a subheading followed by a lengthy discussion of what is and is not "of public or general interest." The section in no way sanctions the use of illegally gotten information. Given the overall tenor of the Warren and Brandeis article, it is difficult to imagine that the authors would have endorsed protecting the redisclosure of a private conversation illegally recorded.

27. *See*, DeVries, *supra* at 288-90 (discussing narrow approach of most privacy statutes and lack of broad legislative solutions)

hands and accepting that we have little or no privacy.

One corporate CEO, Scott McNealy of Sun Microsystems has been routinely quoted as telling an audience "You have zero privacy. Get over it."[28] It does seem that we are increasingly willing to accept McNealy's view of the world by our continued acquiescence and often mindless cooperation with those who seek information about us. How many of us say "no, you cannot have my phone number" when a sales clerk asks for it? Only when the misuse of information about us reaches an egregious level do we seem to sit up and take notice and try to do anything about it.[29] Perhaps this is because in today's modern society it would be almost impossible to get by without participating in activities that create this data.[30] For whatever reason, however, we all seem to acquiescence in the creation of an ever-expanding data trail about us until it is too late to do anything about it.

D. A Judicial Response

In a recent decision the New Hampshire Supreme Court ruled in favor of a plaintiff in a claim for intrusion on privacy rights and did so in manner with potentially broad implications.[31] In *Remsburg v. Docusearch* the executrix of the estate of a murder victim sued an Internet based investigation and information provider which had sold information to the individual who committed the murder. The information included the victim's date of birth, social security number and employment address.[32] That address was obtained by Docusearch through a subcontractor investigator who obtained it by placing a "pretext" telephone call to the victim.[33] The perpetrator used the work address, drove to the victim's workplace, fatally shot her, and then shot and killed himself.[34]

Her estate sued in the United States District Court for the District of New Hampshire which certified five questions to the New Hampshire Supreme Court pursuant to New Hampshire practice.[35] The court issued a number of interesting rulings which will not be addressed in depth in this article. Those included a finding that making a pretextual phone call to acquire address information and then reselling the information constituted a violation of New Hampshire's Consumer Protection Law.[36] In addition, the court made interesting rulings with regard to a restatement claim for intrusion upon seclusion. Specifically, it found that the facts of the case set forth no cause of action for intrusion upon seclusion for the mere act of obtaining address information by way of the pretext phone call. In the court's opinion, where a person works is readily observable by members of the public; the information is not secret, secluded or private, and therefore we have no reasonable expectation of privacy in the location of our employment.[37] The court also ruled, however, that a claim for intrusion upon seclusion could go forward based on the

28. The quote has been used as the lead to at least two articles. *See*, DeVries, *supra* 18 Berkley Tech. L. J. 283; Froomkin, *supra* 52 Stan. L. Rev. 1461. The two authors attribute a slightly different quote McNealy. According to Froomkin the comment was made in response to a question at a Sun Microsystems product launch.

29. Daniel Solove notes in one article that many of us have a general unease about privacy being lost as data is collected about us, but that we have trouble even articulating what causes this feeling. *Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1400 (2000)

30. Solove certainly makes a compelling argument that it is not practical for one to "opt out" of many aspects of modern society which lead to the collection of data about us. *Id. at* 1426 - 28. In contrast, Berman and Mulligan suggest rather cavalierly that many of our problems with information collection can be solved by opting out of the credit card/ATM world and simply using cash wherever we go. Berman and Mulligan, *supra*, at 562.

31. Remsburg v. Docusearch Inc., 816 A.2d 1001; 2003 N.H. Lexis 17 (February 18, 2003)

32. *Id.* at 1005-1006

33. *Id.* at 1006

34. *Id.*

35. The certified questions included whether or not a cause of action existed under the common law for the sale of information, whether or not the sale of a person's social security number could set forth a cause of action for intrusion upon seclusion under the restatement; whether or not obtaining a person's work address and selling it pursuant to a pretextual telephone call could set forth a claim for intrusion upon seclusion under the restatement; whether or not sale of a social security number could set forth a cause of action for commercial appropriation pursuant to the restatement and whether or not obtaining a person's work address pursuant to a pretextual phone call set forth a cause of action under New Hampshire's Consumer Protection Law, New Hampshire RSA Chapter 358-A. *Id.* at 1004, 1005.

36. New Hampshire RSA Chapter 358-A.

37. 816 A.2d at 1009

defendants' conduct with regard to the decedent's social security number. Opining that whether or not the act of disseminating a social security number would be offensive to persons of ordinary sensibilities is a question of fact for the jury, the court allowed the claim to go forward.[38]

The willingness of the New Hampshire Supreme Court to recognize a cause of action for intrusion upon seclusion without a physical violation of the plaintiff's "zone of privacy" is somewhat of a departure from the majority rule.[39] Most of the commentators in this area have been critical of the tendency by most courts considering the issues to require a physical violation of privacy expectations.[40] In that sense, *Remsburg* is a departure from precedent and, arguably, a step forward for those advocating for broader use of the Restatement torts.

The most noteworthy aspect of the *Remsburg* decision, however, is not based on application of a Restatement theory. The first certified question from the District Court to the New Hampshire Supreme Court asks:

> Under the common law of New Hampshire and in light of the undisputed facts presented by this case, does a private investigator or information broker who sells information to a client pertaining to a third party have a cognizable legal duty to that third party with respect to the sale of information?[41]

That question, and the court's analysis of the question is silent as to the restatement torts and the court's analysis in answering that question affirmatively could have extremely broad implications. The court, relying solely on prior New Hampshire decisions considering the question of duty and foreseeability at its most basic levels found that a common law duty flows from an information provider to the person about whom the information is provided even thought the provider does not know what the person seeking information intends to do with it.[42]

The court analyzed the question presented by considering recent New Hampshire decisions broadly relevant to the question of duty, none of which were remotely connected to privacy issues.[43] Recognizing that it would find a foreseeable harm, and thus a duty only rarely in cases involving intervening criminal conduct, the court nonetheless did so.[44] It did so based on commonly recognized privacy considerations, specifically, the risks of stalking and identity theft implicated by information disclosure. The court's analysis was striking in its brevity and simplicity. It leapt from a hornbook treatment of the question of foreseeability to a brief discussion of the societal risks of stalking and information theft and held that:

> The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. And we so hold. This is especially true when, as in this case, the investigator does not know the client or the client's purpose in seeking the information.[45]

38. *Id.*

39. *See e.g.*, Pierson v. News Group Publications, 549 F. Supp. 635 (D.Ga. 1992) ("essential element" of tort of intrusion is physical intrusion analogous to a free pass), Nelson v. Maine Times, 373 A.2d 1221 (Me. 1977) (claim for intrusion should allege physical intrusion upon plaintiff's premises), Froelick v. Werbin, 269 kan. 461, 548 P.2d 482 (1976) (same).

40. *See e.g.*, Froomkin, *supra*, at 1535-37, McClurg, *supra* at 990-1010.

41. Remsburg, 816 A.2d at 1004.

42. *Id.*

43. The New Hampshire Supreme Court cited four decisions in support of its recognition of a duty in Remsburg. Walls v. Oxford Management Co., 137 N.H. 653 (1993) was a case dealing with duties running from a landlord to a tenant with regard to parking lot security. Iannelli v. Burger King Corp., 145 N.H. 190 (2000) concerned the extent to which the operators of a fast food restaurant had a duty to intervene when they observed unruly behavior by teenagers and that behavior eventually escalated into an assault on another patron. Hungerford v. Jones, 143 N.H. 208 (1998) addressed the duty of care owed by a mental healthcare therapist to the parent of the therapist's patient, arising out of allegations that the therapist committed malpractice leading to false accusations of childhood sexual abuse. Dupont v. Aavid Thermal Technologies, 147 N.H. 706 (2002) addressed the duty of care running from employers to employees to prevent criminal attacks by coworkers.

The brief of the plaintiff in the Remsburg case also cites no cases from any other jurisdiction acknowledging a common law tort in such a fact situation. The section of plaintiff's brief relevant to the first certified question is essentially a New Hampshire common law primer on the question of duty and foreseeability.

44. 816 A.2d at 1006.

45. *Id.* at 1008

In short, at the very heart of the New Hampshire Supreme Court's decision is a finding that harm to the party about whom the information being requested is foreseeable where the party providing the information does not know what the requestor intends to do with the information. The court certainly could have justified a ruling that recognizes a duty only where individuals have knowledge that the information will be misused. Its willingness to recognize a duty in a complete void of knowledge opens a potential Pandora's Box when one considers how far that logic could be taken in the current marketplace for information.

Consider, for example, the emerging chip technology that is being used to track product inventory. Warehouse personnel will be trained to use that technology to keep track of where a given product is at a given point in time. Surely the technology is either at a point where it could be abused, or will get to that point in the not too distant future. If a warehouse worker in a hardware chain uses the chip technology to track and stalk a customer will and should the employer of that individual be subjected to liability for the worker's misuse of the technology?

Phone numbers are requested and entered into databases by retailers to compile customer lists. If a store employee uses an individual phone number to do harm to one customer, or uses a collection of phone numbers to target customers for property crimes should the employer be exposed to liability for gathering that information which is later used by an employee bent on such conduct?

Is it "foreseeable" that an employee of an auto manufacturer with access to global positioning satellite technology could use that technology to do harm to the people owning the cars sold by the manufacturers? If that occurs, should the employer be deemed at fault?

These examples are not far flung by any stretch of the imagination. Yet, if one takes the ruling of the Supreme Court to its logical conclusion, is it any more foreseeable that Internet locator information would be misused to do harm than the type of information gathered by the means mentioned above? The New Hampshire Supreme Court's holding is certainly a potential building block for future claims in which aggrieved parties seek to expand tort liability based on a very elemental analysis of the concepts of duty and foreseeablity.

Two authors have already cited *Remsburg* as a major step forward in protecting privacy rights.[46] Those authors, I would suggest, are too eager to embrace the New Hampshire Supreme Court's analysis and do so without careful consideration of the broader implications of Remsburg. The discussion of *Remsburg* by Mark Sweet in the Duke Law And Technology Review is particularly suspect in its advocacy for the proposition that *Remsburg* is a sound decision.[47] Sweet opines that the *Remsburg* decision holds information providers responsible for all conduct by their customers and that this is a positive step in the absence of legislation in the area.

That view is certainly not the only view. If one accepts the New Hampshire Supreme Court's analysis, a party such as Docusearch which has no reason to suspect that the customer in question intends to do harm is *potentially* liable because *possible* harm is "foreseeable." In the current information based world, the logic of *Remsburg* could be extended limitlessly to other areas in which information is available for sale, bought by those with a desire to do harm, and someone attempts to hold the information provider liable after the fact.

---

46. *See* Reidenberg, *Symposium: Enforcing Private Rights: Agency Enforcement And Private Rights Of Action: Privacy Wrongs In Search Of Remedies*, 54 Hastings L. J. 877 (2003) (discussing Remsburg in context of liability for misappropriation of name or likeness); Sweet, *Can The Internet Kill? Holding Web Investigators Liable For Their Criminal Customers*, Duke L. & Tech. Rev. 11 (2003) (discussing Remsburg in context of tort liability for information providers based on conduct of their customers)

47. Sweet's analysis of the Remsburg decision suggests that it is an affirmative finding of liability against Docusearch, implying that the Supreme Court did more than simply recognize the plaintiff's right to present the claim to the jury. In many place, Sweet's analysis reads as if the Supreme Court had entered summary judgment in Remsburg's favor.

E. Conclusion

The manner in which private information is collected and used creates legitimate concerns for all in our society. As technology has advanced the marketplace for information has flourished. Most agree that remedies for breaches or our privacy rights, both statutory and common law, have struggled to keep pace with the expansion of this marketplace.

The New Hampshire Supreme Court's decision in *Remsburg v. Docusearch*[48] reflects an appropriate level of concern with the need to impose responsibility on those who profit from the sale of information about others. Its application of The Restatement (Second) of Torts to recognize a cause of action for intrusion upon seclusion without a physical trespass is a sound decision. Clinging to a physical trespass requirement in such cases is an outdated notion, not in keeping with modern privacy concerns.

A strong argument can be made, however, that the *Remsburg* Court went too far. By recognizing a cause of action not based on a recognized tort or statutory theory, focusing solely on the concept of "forseeability" it may have created too large a stepping stone for future claims. The potential uses and misuses of private information are myriad. The concept of "forseeability" is amorphous and very much in the eye of the beholder. The possible application of *Remsburg*'s analysis are extremely broad and, potentially the opening of a Pandora's Box of tort liabilities.

48. 816 A.2d 1001 (2003).

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

By Rebecca J. Wilson, Christine Filosa and Alex Fennel

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

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

As protection from litigation and potential liability, some employers adopt policies directly addressing dating in the workplace. These policies range from the very strict, such as a comprehensive prohibition of dating between employees, to the more lenient, such as a policy that actively discourages, but ultimately allows, employees to fraternize.[4] Even a simple policy requiring employees to notify management when coworkers are romantically involved provides documentation of a consensual relationship that could be helpful to an employer's defense against a sexual harassment claim, should one arise.[5]

Perhaps daunted by problems of implementation and enforcement, other employers have avoided adopting any formal poli-

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

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

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

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

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

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

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

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

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

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

Employers' Business Interests

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

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

The U.S. Court of Appeals for the Fifth Circuit took guidance from the Supreme Court in *Defenbaugh-Williams v. Wal-Mart Stores* when it held that employers could be vicariously liable for sexual harassment committed by supervisors.[14] One of Wal-Mart's district managers stated during a meeting with other employees that a certain female, the plaintiff employee, "would never move up with the company being associated with a black man." The manager later became the plaintiff's supervisor and instituted a series of disciplinary actions against her on what she alleged were "fabricated workplace-policy grounds," which culminated in her termination. She sued on a theory of sexual harassment.

The court held that Wal-Mart was vicariously liable for the sexual harassment committed by the supervisor. Concluding that the Supreme Court intended to extend prin-

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

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

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

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

10. Mary Stanton, *Courting Disaster*, from Government Executive, October 1, 1998, available at www.govexec.com/features/1098/1098s4.htm (describing dating between supervisors and subordinates as "supervisory suicide"); Labor & Employment in Massachusetts: A Guide To Employment Laws, Regulations and Practices, §§ 5-6 (Matthew Bender and Co. 2001).

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

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

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

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

ciples of agency liability to "all vicarious liability inquiries [brought] under Title VII for acts of supervisors," the court concluded that Wal-Mart was liable for damages based on evidence that the manager had acted with malice or reckless indifference by terminating the plaintiff for having been involved in an interracial relationship.

Such a ruling exposes employers to increased liability for the acts of supervisors in various contexts, which may include the enforcement of anti-fraternization policies. This strict liability under Title VII provides yet another reason for employers to implement these policies with great care and to ensure that their staff is well trained in enforcing the policies.[15]

Another danger is that while two employees are romantically involved in a consensual relationship, neither will claim harassment, but after the romance ends, one party may come forward with the contention that the association was unwelcome, even coerced. This situation presents at least two problems unique to workplace relationships between managers or supervisors and their subordinates, because of the unequal bargaining power of the parties. First, if the subordinate is disciplined, demoted or terminated, he or she may allege retaliation. Second, the party who ended the relationship may bring a sexual harassment claim based on allegations that the other party is forcing him or her to stay in the relationship, stalking or continuing to make unwanted sexual advances, thus subjecting the complainer to sexual harassment. Even if the relationship does not terminate, co-workers may attempt to make a claim against the employer for sexual harassment. That claim may be viable if the employees involved in the relationship repeatedly display sexual favoritism or other inappropriate sexual behavior in the workplace that results in the creation of a hostile work environment.[16]

Even when the relationship does not involve a manager-supervisor and a subordinate, employers still face potential litigation and liability stemming from the romance.[17] Problems can arise, for example, when an employer decides to discipline, demote or terminate a party to a workplace romance even for unrelated reasons. Employees who previously complained of sexual harassment may allege that the disciplinary action was retaliatory. That is, the employee may bring a claim against the employer.[18] The affected employee may also bring a gender discrimination claim, alleging that the employer's action was motivated by favoritism of one gender over another.[19] For example, in *Russel v. United Parcel Service*, a female supervisor was terminated for living with an hourly employee in violation of a company policy prohibiting anti-fraternization. The discharged employee sued her employer alleging discrimination on the basis of her gender and sexual orientation because women were disciplined differently than men for violations of the employer's anti-fraternization policy. In Russel, the Court of Appeals of Ohio held that the record was sufficient to create a material issue of fact which precluded summary judgment for the employer. [20]

Based on this potential legal liability and a reasonable desire to maintain a productive staff, an employer has a legitimate business interest in drafting rules and regulations that will help it to avoid the myriad of problems that office romances can create.[21] For instance, if an employer prohibits its super-

15. Kramer, *supra* note 5, at 120; Tara Kaesebier (Comment), *Employer Liability in Supervisor Sexual Harassment Cases: The Supreme Court Finally Speaks*, 31 ARIZ. ST. L.J. 203, 223 (1999).

16. *See* for this paragraph Kramer, *supra* note 9, at 87-94; Stanton, *supra* note 10; Mann, *supra* note 12; Dean, *supra* note 4, at 1054.

17. Meyer, *supra* note 2.

18. Kramer, *supra* note 9, at 96.

19. *See* Sanguinetti v. United Parcel Service, 114 F.Supp.2d 1313 (S.D. Fla. 2000) (male supervisor terminated for violating employer's no-dating policy sued for gender discrimination where female manager who violated policy was not terminated).

20. Russel v. United Parcel Service, 110 Ohio App.3d 95, 673 N.E.2d 659, 71 A.L.R. 5th 741 (1996); *But see*, Shumway v. United Parcel Service, 118 F.3d 60 (2nd Cir. 1997) (Summary judgment properly allowed against employee claiming sex discrimination who admitted violating anti-fraternization policy where employee failed to show that male employees who violated same policy were treated differently.)

21. Kramer, *supra* note 9, at 79.

visors from dating their subordinates, it may be less likely to face a quid pro quo sexual harassment charge. Similarly, if a company requires its employees to sign acknowledgement or consent forms when they enter into a romantic relationship with a coworker, they will have documentation on file to defend themselves from liability if a claim against them is later brought.[22] However, these rules, intended to shield employers from litigation, may, ironically, give rise to other forms of liability when an employer enforces them. When an employee is subjected to an adverse action in connection with their job for a violation of an anti-fraternization policy, the employee may challenge the employer's rules regarding employee relationships, arguing that the regulations constitute an invasion of privacy.[23]

Employees' Privacy Interests

At the heart of employees' interests in engaging in consensual workplace relationships lies their rights to privacy. In its original form, the constitutional right to privacy protected individuals from improper acts of government officials.[24] Since its recognition in the 1950s, however, the constitutional right to privacy has grown to encompass the autonomy individuals enjoy in making certain kinds of decisions, especially those of a particularly personal nature. Personal decisions likely to be protected by this right to privacy include issues surrounding marriage, procreation, contraception, child-rearing and education.[25] The right to privacy also protects the right of individuals to be free from governmental surveillance and intrusion in their private affairs.[26]

Every state in the United States now recognizes "some general form of common law protection for privacy."[27] Public sector employees in several states also enjoy state constitutional protection of a general privacy right.[28] Florida's constitution limits the ability of government employers to invade the privacy of their employees.[29] Texas courts have held that the Texas Bill of Rights protects "personal privacy from unreasonable intrusion" and have extended this protection to the rights of public sector employees.[30] In California, employees may invoke a public policy exception to at-will employment termination by asserting a violation of their privacy right under the state constitution.[31]

In addition to these more conventional forms of protection, more than half the states have legislation protecting employee privacy with regard to activities conducted outside the workplace.[32] In Colorado, North Dakota and New York these laws are general enough to protect almost all legal activities not related to an individual's employment. New York's, for instance, extends quite broadly to protect the "legal recreational" activities of employees.[33] Colorado's states that it is an unfair employment practice to discriminate against employees for engaging in "lawful activities," either outside of the office or while working.[34] North Dakota's makes it unlaw-

22. Maharaj, *supra* note 1.

23. Dean, *supra* note 4, at 1058; Kramer, *supra* note 9, at 105.

24. William M. Beaney, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212 (1963) (discussing the meaning of the constitutional right to privacy).

25. Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925) (extending constitutional right of privacy to child rearing and education); Prince v. Massachusetts, 321 U.S. 158 (1944) (extending constitutional right of privacy to decisions regarding family relationships); Skinner v. Oklahoma ex. rel. Williamson, 316 U.S. 535 (1942) (extending constitutional right of privacy to procreation); Loving v. Virginia, 388 U.S. 1 (1967) (extending constitutional right of privacy to marriage); Griswold v. Connecticut, 381 U.S. 479 (1965) (extending constitutional right of privacy to contraception); Roe v. Wade, 410 U.S. 113 (1973) (extending constitutional right of privacy to abortion).

26. Bruce L. Watson, *Disclosure of Computerized Health Care Information: Provider Privacy Rights Under Supply Side Competition*, 7 AM. J. L. AND MED. 265, 269 (1981), citing Roe.

27. Michael Z. Green, *A 2002 Employment Law Odyssey: The Invasion of Privacy Tort Takes Flight in the Florida Workplace*, 3 FLA. COASTAL L.J. 1, 9 (2001).

28. Helen M. Richards, *Is Employee Privacy an Oxymoron?* 15 DELAWARE LAW. 20, 20-21 (1997).

29. Green, *supra* note 26, at 14.

30. Texas State Employees Union v. Texas Dep't of Mental Health and Mental Retardation, 746 S.W.2d 203 (Tex. 1987).

31. Semore v. Pool, 1990 Cal.App. LEXIS 94.

32. Alison J. Chen (Note), *Are Consensual Relationship Agreements a Solution to Sexual Harassment in the Workplace*, 17 HOFSTRA LAB. & EMP. L.J. 165, 188 (1999).

33. N.Y. LABOR LAW § 201-d (2002).

34. COLO. REV. STAT. ANN. § 24-34-402.5.

ful to hire or fire an employee for engaging in a "lawful activity outside work" that does not interfere with the employer's business interests.[35]

Anti-Fraternization Policies: Balancing Competing Interests

A. Public Sector Employees

The liberty that employers have to limit the activities of employees varies depending on whether they operate in the public or private sector. There are significant differences between these two arenas as they relate to the regulation of romantic involvement in the workplace.

State and federal constitutional provisions that explicitly protect individual privacy rights apply only to state actions.[36] When the state is the employer, it may not, without substantial justification, condition employment on the relinquishment of constitutional rights, but it nevertheless has greater latitude in restricting the activities of its employees than it has in regard to the activities of its citizens at large.[37] Accordingly, public sector employees generally enjoy a more rigorously protected right of privacy than do employees in the private sector. The courts must carefully consider both the interests of the individual and the interests of the government when determining whether the private activities of a public employee constitute valid grounds for action.[38]

Apparently aware of the intricacies of these issues, the U.S. District Court for the Eastern District of Missouri opined in *Wieland v. City of Arnold* that it was "uncomfortable" adopting a general rule that all dating relationships are constitutionally protected, especially for government employees working in "sensitive areas" of law enforcement.[39] In that case, a police officer challenged a city's police department regulation prohibiting unbecoming conduct violated, among other things, his right to privacy.

The chief of police had ordered the plaintiff to end his relationship with a woman who was on probation for a felony offense. The plaintiff had appeared at a city ribbon-cutting ceremony with the woman, and a picture of the two at the ceremony appeared in a local paper. The chief thought that this public appearance both embarrassed the city and violated a general order of the department "forbidding as unbecoming conduct . . . [k]nowingly associating, on or off duty, with convicted criminals or lawbreakers under circumstances which could bring discredit upon the department or impair an Officer in the performance of his duty."

The court held that although the plaintiff's relationship with a convicted felon did not impact his job performance, it was not "unreasonable to assume a very real likelihood that it could affect the chain of command as well as the public image of the department." The court ultimately concluded that while such "looser socialties" as dating may be protected, they receive less stringent protection from privacy laws than other, more formal associations might enjoy.

Relying in the reasoning in *Weiland v. City of Arnold* that the interests of a police department, as a paramilitary organization, outweigh an individual officer's right to privacy, the United States District Court for the Northern District of Iowa recently affirmed the grant of summary judgment for a public employer which terminated a probationary police officer involved in an extra-marital affair with a police captain. In *Mercer v. City of Cedar Rapids*, the Court held that inquiries into a police officer's off-duty romantic relationship with a superior officer and termination of her employment because of this relationship, even in the absence of a non-fraternization rule, would not constitute an invasion of privacy given the department's interest in maintaining order and public confidence in the department. [40]

35. N.D. CENT. CODE § 14-02.4-0.8 (1997).

36. Born v. Blockbuster Video Inc., 941 F.Supp. 868, 870 (S.D. Iowa 1996).

37. Briggs v. North Muskegon Police Dep't, 563 F.Supp. 585, 587 (W.D. Mich. 1983) (citations omitted).

38. Dean, *supra* note 4, at 1058; Kramer, *supra* note 9, at 106.

39. 100 F.Supp.2d 984, 988 (E.D. Mo. 2000).

40. Mercer v. City of Cedar Rapids, 104 F.Supp.2d 1130 (N.D. Iowa 2000).

In *Shawgo v. Spradlin*,[41] the Fifth Circuit specifically noted that the right to privacy does not come without qualification and that the state has a greater interest in regulating the activities of its employees than it has in regulating the activities of the general population. In *Shawgo*, two former police officers sued a city and others for an alleged invasion of privacy resulting from the disciplinary action taken against them for dating and allegedly cohabitating in violation of department regulations. One officer was a patrolwoman and the other a sergeant. The patrolwoman did not report directly to the sergeant, so the problems common to romantic relationships between managers or supervisors and their subordinates did not arise.

Finding a rational connection between the "exigencies of department discipline and [the rule] forbidding members of a quasi-military unit, especially those different in rank, to share an apartment or to cohabit" the court nevertheless concluded that the policy did not offend the plaintiffs' privacy rights. It went on to hold that the investigatory surveillance of the employees' off-duty association in violation of department regulations did not impinge upon the right to privacy.

Similar cases have reached consistent outcomes where the relationship is between a government employee and a non-government employee. In Briggs v. North Muskegon Police Department, the federal district court for the Western District of Michigan concluded that a city violated a police officer's privacy rights when it dismissed him for cohabitating with a woman while separated from his wife.[42]

A police officer's right to privacy also was violated in *Shuman v. City of Philadelphia* when the police department fired him for living with a married woman who was not his wife.[43] Similarly in *Via v. Taylor*, the United States District Court for the District of Delaware found that a correctional officer's right to privacy was violated when she was fired as a result of an off-duty relationship with a former inmate in contravention of her employer's code of conduct. In so doing, the Court recognized that privacy rights of public employees should be evaluated under an intermediate scrutiny standard of review. In applying this standard of review to the regulation in issue, the Court concluded that it failed to pass constitutional muster.[44] In contrast, however, recall that Wieland held that a city's order to a police officer to terminate his relationship with a known felon pursuant to a policy forbidding association with a convicted criminal did not violate the police officer's right to privacy.

Since their employees possess somewhat stronger rights of privacy in the workplace than do their counterparts in the private sector, employers in the public sector should exercise caution when structuring anti-fraternization policies.[45] Relevant case law indicates that courts will evaluate anti-fraternization policies of government employers relative to the type of work involved, the existence of superior-subordinate relationships and whether one of the two employees directly reported to the other.

B. Private Sector Employees

Private sector employees receive protection from invasions of privacy under state legislation and common law. Several states have adopted laws protecting all legal off-duty activities, provided they do not directly conflict with an employer's legitimate business interest.[46] Private sector employees, however, have very few privacy rights that protect them within the workplace. To prevail on an invasion of privacy claim, there must exist a reasonable expectation of privacy in the matter at issue. Under this standard, if employees have advance notice of a company anti-fraternization rule, their claim is substantially weakened.[47] An

41. 701 F.2d 470, 482-83 (5th Cir. 1983). 1 Id. at 472.
42. 563 F.Supp. 585 (W.D. Mich. 1983).
43. 470 F.Supp. 449 (E.D. Pa. 1979).
44. Via v. Taylor, 224 F.Supp.2d 753 (D. Del. 2002).
45. Dean, *supra* note 4, at 1058.
46. Ann H. Zgrodnik (Comment), *Smoking Discrimination: Invading an Individual's Right to Privacy in the Home and Outside the Workplace?* 21 OHIO N.U.L. REV. 1227, 1244-45 (1998).
47. Kramer, *supra* note 9, at 120, 129.

employee who knowingly violates an anti-fraternization rule cannot be said to have had a reasonable expectation of privacy in the matter.

In *Rogers v. International Business Machines Co.*,[48] the employer dismissed a manager for having an alleged relationship with a subordinate that "exceeded normal or reasonable business associations, [and] negatively affected the duties of his employment." The employer had no policy or rule prohibiting such relationships, and the manager claimed that his termination was improper because it was predicated on an investigation of a personal matter, which invaded his right of privacy.

The U.S. District Court for the Western District of Pennsylvania concluded that the employer acted reasonably, noting that nothing on the record indicated any impropriety and that in fact the manager had participated in the investigation and had received timely notice of his termination. In support of its decision, the court cited what it described as the employer's legitimate interest in "preserving harmony among its employees and . . . preserving normal operational procedures from disruption."[49] The court also rejected the plaintiffs' tort claim for invasion of privacy. It underscored the fact that the employer had limited its investigation to interviews with employees and to an examination of company records, and it concluded that the employer had not intruded on the plaintiff's "seclusion or private life."

Similarly, in *Watkins v. United Parcel Service*,[50] the employer fired a manager for violating the company's anti-fraternization policy by having a romantic relationship with a U.P.S. truck driver. The manager claimed the company's conduct was "highly offensive" because his personal relationship with the driver did not concern the company because it occurred primarily off the job. He also alleged that he and the co-worker had contemplated marriage and that his discharge prevented that marriage from coming to fruition.

The U.S. District Court for the Southern District of Mississippi rejected the claims and found at least partial support for its decision in the manager's failure to provide, or even allege, an "utterly reckless" invasion by the company, such as snooping in his bedroom or electronically wiring his workspace.

In *Patton v. J.C. Penney Co.*,[51] a former employee sued for wrongful discharge and intentional infliction of emotional distress after being terminated for dating a co-worker. One of the employer's supervisors had told the plaintiff to end his "social relationship" with a female co-worker. The plaintiff responded by saying that he did not socialize while working and that he would continue to see the co-worker during his own time. The supervisor later told the plaintiff that his job performance was not satisfactory and that he would be fired if his performance did not improve. The plaintiff employee asked to be transferred to another department, but the supervisor denied his request, and he ultimately was terminated for unsatisfactory job performance.

In affirming the lower court's judgment for the employer, the Oregon Supreme Court held that the dismissal did not violate public policy and did not amount to "outrageous" conduct.

In a similar case, *Sarsha v. Sears Roebuck & Co.*,[52] the plaintiff employee, a supervisor, was fired for dating a subordinate employee, who, however, was not fired. The plaintiff sued, alleging age discrimination in violation of the Age Discrimination in Employment Act, and a gender discrimination claim in violation of Title VII. In rejecting the claims, the Seventh Circuit ruled that the employer was "entitled to enforce a non-dating policy . . . against [its] supervisors, who by virtue of their managerial positions are expected to know better."

48. 500 F.Supp. 867, 868 (W.D. Pa. 1980).
49. Quoting Geary v. U.S. Steel Corp., 319 A.2d 174, 178 (Pa. 1974).
50. 797 F.Supp. 1349, 1351 (S.D. Miss. 1992).
51. 719 P.2d 854 (Or. 1986).
52. 3 F.3d 1035, 1037 (7th Cir. 1993).

Nevertheless, to be upheld, an employer's anti-fraternizations policies must be enforced consistently and in a gender-neutral manner. For instance, in *Zentiska v. Pooler Motel Ltd.*,[53] the employer ordered one of its supervisors either to quit his job or fire the plaintiff employee whom the supervisor was dating. The supervisor removed plaintiff employee's name from the work schedule. One of the employer's area directors, however, had dated and ultimately married a co-worker. The employer had not enforced its anti-fraternization policy with respect to that situation. The area director not penalized was male; the plaintiff who was fired was female. The federal district court in Georgia found the defendant liable for sex discrimination on the ground that it had treated the female plaintiff differently from a similarly situated male employee.

Courts that have encountered these issues have consistently decided in favor of the proposition that employers must act reasonably and consistently, both in the implementation and the execution of anti-fraternization policies.[54] For instance, in Watkins, the plaintiff did not argue that the anti-fraternization policy itself constituted an invasion of privacy, but rather that the investigation into the relationship violated his privacy rights. As that case demonstrates, the manner in which a company enforces its anti-fraternization policy is equally important to an employer seeking to avoid litigation as the policy itself.

Employers who adopt anti-fraternization policies appear to be fairly well protected from liability on invasion of privacy grounds, so long as the policy and its implementation are reasonable.[55] Courts have demonstrated sympathy for the plight of employers facing problems arising from fraternization between employees. They recognize that workplace romances can have a tangible and often negative impact on a company's ability to achieve legitimate business objectives. At the same time, however, courts maintain a clear respect for the individual privacy rights of employees and will not allow those rights to be abrogated beyond reason.[56]

To arm themselves against various kinds of liability, employers should craft policies that are reasonable in scope and degree and that can be fairly and consistently enforced. A reasonable policy will focus on the effect the relationship has on the business interests of the employer. For example, there should be some correlation between the romantic relationship and the employees' performance on the job. It likely will be more difficult to defend an anti-fraternization policy relating to the activities of employees outside the workplace if the policy does not require that the outside activity impact a legitimate business objective or interest.

C. Off-duty Conduct

Another important issue that arises in cases involving romantic relationships at work centers around the highly controversial idea that employers have the ability and also the right to regulate the activities of their employees outside the workplace. The best-known case on this issue involves two former employees of Wal-Mart, *New York v. Wal-Mart Stores*.[57] Both were terminated for violating the company's fraternization policy, which prohibited a "dating relationship" between a married employee and another employee, other than his or her own spouse.

In an action seeking the re-instatement of the terminated employees, the New York Attorney General argued that the firing violated a New York statute that made it unlawful for any employer to "refuse to hire, employ, or license or to discharge from employment or otherwise discriminate against an individual . . . because of . . . an individual's legal recreational activities outside work hours, off the employer's premises and without use of the employer's equip-

53. 708 F.Supp. 1321, 1322-25 (S.D. Ga. 1988).

54. *See* Sanguinetti v. United Parcel Serv., 114 F.Supp.2d 1313 (S.D. N.Y. 2000) (dismissing invasion of privacy claim brought by employee fired for violating no-dating rule).

55. Kramer, *supra* note 9, at 78, 96.

56. Michael Dworkin, *It's My Life--Leave Me Alone: Off-the-Job Employee Associational Privacy Rights*, 35 AM. BUS. L.J. 47, 95 (1997).

57. 621 N.Y.S.2d 158 (App.Div. 3d Dep't 1995).

ment or property."[58]

The outcomes of cases interpreting this statute have hinged almost entirely on the courts' interpretation of the phrase "recreational activities." In the *Wal-Mart* case, the trial court had found that the employees may have engaged in recreational activities while dating and that the fact that they engaged in these "protected leisure activities . . . together did not vitiate their statutory protection." The Appellate Division, however, reversed, holding that "dating" is distinct from and, in fact, bears no resemblance to "recreational activity." The employees could not receive protection under the statute.

Critics of the court's reasoning, however, have argued that this interpretation of the statute "overlooks [its] essential purpose, which is to protect employees' off-the-job activities so long as they [do not bear]" on one's job performance.[59] In contrast, a New York federal district court's interpretation of the same language concluded that cohabitation qualified as a recreational activity under the statutory scheme.[60] The court relied on the statute's legislative history, which it held reflected a "general policy of protecting employees from discrimination" against employees who happen to engage in activities after work that their employer does not like.

Many states have adopted these off-the-job privacy laws in some shape or form, indicating that this type of statute will remain a force to be reckoned with as employers confront the issue of romantic relationships in the workplace and draft anti-fraternization policies.[61] Ultimately, it appears that the outcome of these cases will depend on the legislative history of the statutes involved and how courts decide to interpret the relevant statutory language.

D. Privacy on the Internet

Another related issue is whether employees have an expectation of privacy with regard to e-mails sent or received on an office computer system. For instance, an employer might discover that its employees are fraternizing in violation of a company policy by intercepting a related e-mail message. In *Restuccia v. Burk Technology Inc.*,[62] the Massachusetts Superior Court held in 1996 that employees do not have a reasonable expectation of privacy regarding e-mails sent and received at work and that, therefore, an employer did not violate the state wiretapping law when it stored and reviewed messages from a company server.

More recently, the U.S. District Court for the District of Massachusetts held that even where employees may have a reasonable expectation of privacy in their office e-mail, the legitimate business interests of their employers will likely trump employee privacy interests. In *Garrity v. John Hancock Mutual Life Insurance Co.*,[63] that court noted that both Title VII and state law require employers take proactive steps to eliminate harassment from their offices and to investigate any potentially harassing conduct when this conduct is brought to their attention.

Similarly, in *Smyth v. Pillsbury Co.*,[64] the federal district court in the Eastern District of Pennsylvania held that pursuant to Pennsylvania law, an employee fired for making disparaging comments on an e-mail written at work did not have an expectation of privacy in this communication. In *McLauren v. Microsoft Corp.*[65] a Texas Court of Appeals held that an employee did not have a reasonable expectation of privacy in the contents of an e-mail message that he had saved to a "personal" file.

Thus, it appears that an employer who discovers a violation of its fraternization

58. N.Y. LABOR LAW § 201-d.

59. Dworkin, *supra* note 54, at 53-54.

60. Pasch v. Katz Media Corp., 1995 WL 469710 (S.D. N.Y.); *But see*, McCavitt v. Swiss Reinsurance America Corp., 89 F.Supp.3d 495, 499 (S.D. N.Y. 2000) (where a different judge of the United States District Court for the Southern District of New York concluded that a dating relationship would not be under the protection of the statute).

61. Dworkin, *supra* note 54, at 55; Dean, *supra* note 4, at 1067 nn. 114-115.

62. 1996 Mass.Super. Lexis 367 (1996).

63. 2002 U.S.Dist. Lexis 8343 (D. Mass.).

64. 914 F.Supp. 97, 101 n.3 (E.D. Pa. 1996).

65. No. 05-97-00824-CV (Tex.App. 1999), unpublished but available at http://www.5thcoa.courts.state.tx.us/cgi-bin/as_web.exe?c05_99.ask+D+10706510.

policy by intercepting an e-mail sent on an office system does not violate the privacy rights of the employees involved in acting on knowledge acquired via the intercepted message.

Crafting Anti-Fraternization Policies

A well-drafted, carefully implemented and widely disseminated corporate policy regarding fraternization among employees can provide substantial legal protection to employers.[66] The employer must first determine the nature of the limitation desired and then decide how it will enforce the policy. The policy should provide a precise definition of the discouraged, limited or prohibited conduct. For example, an employer may define the phrase "personal relationships" to encompass romantic relationships as well as family relationships or relationships with the potential for conflicts of interest.

The employer also must determine the extent to which the policy will limit such relationships. One might choose to adopt a comprehensive policy prohibiting all relationships between co-workers. Another, believing this too restrictive, might opt to limit the prohibition to personal relationships between a manager and a subordinate, with or without providing various other qualifications such as whether the subordinate reports directly to the supervisor. An even less restrictive option would be a limitation on a manager's ability to have a "personal relationship" with a subordinate within his or her chain of command.

Finally, the employer must consider the types of consequences it will apply to employees who violate the policy. These may include transfers to another department, termination, reprimand or demotion. Employers should carefully consider not only the potential reaction of its employees to the policy, but also the practicality and difficulty of enforcing it, given its business circumstances. In the end, for an anti-fraternization policy to survive claims brought on privacy grounds it must strike a reasonable balance between the interests of the employer and the interests of the employees.

An employer or advising attorney wishing to avoid claims that a policy violates the privacy rights of its employees should structure the policy around the impact potential romantic relationships at work may have on job performance. This will increase the likelihood that a court will find a rational connection between the policy and the achievement of legitimate business objectives. The more specific the policy is in defining its prohibitions and the scope of their application, the more notice employees will be seen to have had. The more notice employees have regarding their employer's anti-fraternization policy, the weaker their argument that they had a reasonable expectation of privacy regarding the romantic relationship.

Conclusion

The privacy rights of employees typically do not prohibit employers from acting as the dating police by implementing or enforcing a policy against romantic relationships in the workplace. In many, if not most instances, the employer's legitimate business interests in maintaining a peaceful and productive work environment and

66. For references to this section, see Kramer, *supra* note 9, at 78, 120; Dean, *supra* note

avoiding liability outweigh an employee's right to privacy. This has proved to be especially true in the context of an employment relationship in the private sector.

If an employer decides to promulgate rules and regulations regarding office romances, the policy should not intrude on employees' private affairs unreasonably and should display respect for the personal lives of employees, while also protecting the employer's interest in avoiding the many problems that can result from these romances. The policy should be stated clearly and tailored narrowly to protect the employer's legitimate business interests. Consideration may be given to restricting only relationships between supervisors and subordinates since in the past these relationships have been the most likely to lead to litigation because of the imbalance of power between the two parties, as well as being the most likely to affect job performance. Most critically, whatever form of policy an employer chooses to adopt, it must enforce the policy in a uniform and non-discriminatory manner.