The Joan Fullam Irick Privacy Project, Phase III

Dedication

It's hard to believe that it has been four years since Joan Irick passed away. She brought so much talent, imagination, strength and courage to the IADC and, along with her husband, Tom, represented what was so special about the experience of active IADC membership.

In trying to come up with an appropriate ***"Dedication"*** for Phase III of her ***Privacy Project***, we realized that, although so much has changed over the past four years, Joan's inspiration and dreams for this venture are just as strong as ever today.
In the hopes of allowing some of you who did not have the privilege and opportunity of knowing Joan to learn a bit about her, we decided to reprint a portion of the ***Dedication*** in Phase II written so briefly after her passing.

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 eventually lost her battle with cancer but her spirit remains with us in many ways. Perhaps the most visible is the ongoing relationship of her husband, Tom Irick, with the IADC and so many of its members. Tom continues to play a very active role in most IADC Midyear and Annual Meetings and has retained so many friendships that the Iricks generated over the years.

In recognition of all that Joan and Tom Irick brought to and did for the IADC and to recognize Tom's continuing active role, we dedicate Phase III of the Privacy Project to Tom Irick.

Editors
George Hodges, Jerry Galante, Joe Ryan, and Eric Wiechmann

The Joan Fullam Irick Privacy Project, Phase III

In 2001, Joan Irick submitted a proposal 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 Executive Committee 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 IADC members and future IADC Board members Joseph W. Ryan, Jr. and Jerome A. Galante.

A strategy 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 IADC 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. Phase II was published in January 2004 - several months after Joan Irick passed away. Now that a few years have passed and privacy issues have become more complex, better defined and in some cases changed, the IADC Foundation decided the publication of Phase III would be an appropriate supplement to the past volumes.

The previous Editorial Team of George Hodges, Jerry Galante and Joe Ryan were joined by IADC Board member and Past Foundation President, Eric Wiechmann, in overseeing the creation of this newest phase.

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 Joe Blaszynski and Mary Beth Kurzak of the IADC staff, whose multi-task efforts made this project possible and the IADC Foundation for its support.

Table of Contents

IADC
International Association of Defense Counsel

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

The Foundation
of the International Association of Defense Counsel

The Cycle of America's Privacy Intrusion: The USA Patriot Act Continues A Historical Trend

By: Rebecca J. Wilson and Eric R. LeBlanc

I. Introduction

Throughout the history of the United States, events threatening national security have served as a catalyst for governmental intrusion into personal privacy. The events of September 11, 2001 ("9/11") were no different in terms of bringing about increased scrutiny into the privacy of the average citizen. By passing the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" ("USA Patriot Act") in 2001[1], the United States Government was merely following a pattern established and repeated in past generations. The fact that the USA Patriot Act infringes on some aspects of personal privacy formerly enjoyed by United States citizens is not a novel concept in responding to times of alleged national crisis. In fact, the passing of the USA Patriot Act merely serves to reinforce the historical ebb and flow of governmental intrusion into the privacy of its citizens.

Interestingly, this natural progression of privacy intrusion is mirrored by the sentiments of the citizens it affects. In the immediate aftermath of 9/11, the average United States citizen felt a need for greater security and protection from terrorist activity. This need for protection manifested itself through large scale acquiescence to the Government's actions in the few months directly following the attacks. In order to realize this need for security, the general public, through their representatives in Congress, were willing to support the passage of the USA Patriot Act and accept its detrimental effects on their personal privacy.[2] Now, almost five and half years after the attacks of 9/11, the general public is slowly beginning to resent its loss of privacy[3]. The US Congress acknowledged this increasing resentment by passing a permanent but less intrusive version of the USA Patriot Act on March 9, 2006.[4] If past trends are accurate

IADC member Rebecca J. Wilson is a partner in the Boston office of Peabody & Arnold LLP where she concentrates her practice in employment litigation and employment practices counseling. She received her undergraduate degree from Trinity College in Washington, D.C., and her law degree from Boston College in 1979.

Eric R. LeBlanc is an associate in the same firm. He graduated from Boston College in 2003 and received his J.D. from Suffolk University Law School in 2006.

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intersect and Obstruct Terrorism Act (USA Patriot Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[2] According to a Gallup Poll taken on June 21-23, 2002, 85% of citizens asked whether the US Government's actions in response to terrorism went too far answered that the Act was a necessary tool that either used about the right amount or not enough privacy intrusion, whereas only 11% said the Government's actions went too far. http://www.galluppoll.com/content/?ci=5263&pg=1 (last visited February 13, 2007).

[3] According to a Gallup Poll taken on May 12-13, 2006, only 53% of respondents stated that the US Government's intrusion was about right or not enough, whereas 41% of respondent's stated the Government's actions went too far. http://www.galluppoll.com/content/?ci=5263&pg=1 (last visited February 13, 2007).

[4] The United States Senate voted to renew the Act on March 2, 2006. On March 7, 2006, the House

indicators, absent another catastrophic terrorist event, chances are that public outcry regarding The Patriot Act's intrusion into privacy will continue to mount and create legislative and judicial change.

While some may feel that the USA Patriot Act's intrusion on citizens' privacy is unprecedented, the degree of intrusion is no greater than during past instances of national crisis. Though different in scope and content than past historical measures, the USA Patriot Act does not supersede past instances of governmental intrusion of privacy. The main difference between historical privacy intrusions and those permitted by the USA Patriot Act is rooted in the technological differences between the times. Where in the past the Government would physically monitor an individual's membership in what it deemed subversive groups through clandestine monitoring, nowadays the advent of the internet and sophisticated wiretapping devices allow the Government to monitor its citizens through more secretive methods. This type of intrusion, though troubling, should not be considered any more insidious or invasive than past efforts. Just because the Government's surveillance techniques are more sophisticated and less apparent does not mean that they are more invasive.

The USA Patriot Act was enacted with the stated aim of "protecting" the public from future terrorist activity. Like other periods in history where the United States Government enacted laws facilitating intrusion on citizens' privacy, the federal Government used the public's fear and perception of imminent danger post-9/11 to gain acceptance of the Patriot Act. Be it World War II, the era of McCarthyism or the Cold War, or even as far back as the Civil War, the Government has been quick to take advantage of an opportunity to exploit on the fears of its citizens. The United States Government has long understood the powerful effect of fear and the way that it blinds a citizen from perceiving and challenging a forfeiture of civil liberties, most notably privacy. Even though our Government may be acting with good intentions (i.e. "protecting" its citizens from danger), it consistently abridges personal privacy in times of perceived danger. By enacting the USA Patriot Act after the events of 9/11, the United States Government followed a well established pattern of abridging individual freedom in the face of perceived threats to our national security.

This article will: (I) Describe the USA Patriot Act's effect on privacy in the U.S.; (II) Survey the history of privacy intrusion in the United States during times of enhanced national security, and; (III) Forecast the future impact of the US Patriot Act using the historical landscape as a backdrop. The article will also examine recent case law challenging the USA Patriot Act as well as past decisions affecting privacy rights of United States citizens during times of national crisis.

II. The History Of Privacy Intrusion In The United States

A. Historical Times of National Crisis Where Privacy Has Been Intruded Upon By the United States Government

i. Alien and Sedition Acts of 1798

In response to a threat of war with France, the United States Government passed four separate pieces of legislation which as a whole constituted the Alien and Sedition

---

gave its final vote in approval of renewing the act. The legislation to extend the statute will make all but two of its provisions permanent. The provisions in question are the authority to conduct "roving" surveillance under the Foreign Intelligence Surveillance Act ("FISA") and the authority to request production of business records under FISA (USA PATRIOT Act sections 206 and 215, respectively). These provisions will expire in 4 years. *See* USA PATROT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (March 9, 2006).

Acts of 1798.[5] The first of the four laws was the Naturalization Act which extended the amount of time required for aliens to become citizens of the United States from five years to fourteen years.[6] The second law, the Alien Friends Act, authorized the Government to deport any alien it felt was "dangerous to the peace and safety of the United States."[7] The third act, and the only part of the Alien and Sedition Acts of 1798 remaining in effect today, was the Alien Enemies Act which allowed the Government to detain and deport any aliens whose country of origin was currently at war with the United States.[8] And finally, the Sedition Act made it a crime for anybody to publish "false, scandalous and malicious writing" against the Government.[9] On their face, these acts do not seem to be an affront to a citizen's right to privacy; however, the methods the Government used to enforce these acts were clearly similar to the types of intrusion authorized by today's USA Patriot Act. By 1802, these laws, except for the Alien Enemies Act, were repealed amid large scale protest and Presidential change, but they truly were the first instance and quite possibly the birth of the United States Government's cycle of privacy intrusion.

ii. Civil War

The United States Civil War is yet another time of national crisis when the United States Government intruded upon the privacy rights of its citizens. Directly upon the outbreak of the Civil War, President Abraham Lincoln declared a national state of emergency and suspended all individual rights in key border states.[10] Further, Lincoln detained 13,000 civilians and in doing so suspended the writ of habeas corpus so there could be no inquiry into the reasons behind their detainment.[11] Lincoln's actions were taken under his war-time powers as President of the United States and virtually tied the hands of many dissenters.[12] In addition to Lincoln's exercise of Presidential war powers described above, U.S. privacy rights were abridged for tactical reasons by other groups within the Government. The Government freely used census data to help prepare war strategy and, further, "General Sherman used census data to locate targets during his famed Civil War March through Georgia."[13] Clearly, the measures taken by Lincoln, and this obvious misuse of census data by the armed forces, represented invasions of privacy as aggressive as those authorized by the USA Patriot Act. By the end of the war, many of these intrusions on personal privacy rights had ceased because Lincoln could no longer invoke his emergency powers, but before that happened, there were considerable calls for change from the U.S. public. These events clearly follow the cycle of the imposition and lifting of intrusions into privacy that was first demonstrated by the passage and

[5] Text of all four separate pieces of legislation making up the Alien and Sedition Acts of 1798 available at http://www.loc.gov/rr/program/bib/ourdocs/Alien.html (last visited February 20, 2007).

[6] Naturalization Act available at http://memory.loc.gov/cgi-bin/ampage?collId=llsl&filename=001/llsl001.db&recNum=689 (last visited February 20, 2007).

[7] Alien Friends Act available at http://memory.loc.gov/cgi-bin/ampage?collId=llsl&filename=001/llsl001.db&recNum=693 (last visited February 20, 2007).

[8] Alien Enemies Act available at http://memory.loc.gov/cgi-bin/ampage?collId=llsl&filename=001/llsl001.db&recNum=693 (last visited February 20, 2007); The Alien Enemies Act remains law today at 50 U.S.C.A. §§ 21-24.

[9] Sedition Act available at http://memory.loc.gov/cgi-bin/ampage?collId=llsl&filename=001/llsl001.db&recNum=719 (last visited February 20, 2007).

[10] These states were Maryland, Kentucky, Missouri, and Tennessee. *See* Bruce Catton, *This Hallowed Ground: The Story of the Union Side of the Civil War*, (1956).

[11] *See Id.* at 28.

[12] *Id*.

[13] *See* The Census and Privacy, available at http://www.epic.org/privacy/census/ (last visited February 16, 2007).

subsequent repeal of the Alien and Sedition Acts.

iii. U.S. Internment of Japanese Americans During World War II

During World War II, the United States Government forcibly removed approximately 110,000 Japanese-Americans from their homes on the West Coast of the United States and detained them in internment camps.[14] The detentions started December 8, 1941 and lasted over a year.[15] The Government did not require Japanese Americans to be a threat to national security in order to detain them; the mere fact of their race was enough to have them detained. See *Korematsu v. United States*, 323 U.S. 214, 217-19 (1944). The largest privacy intrusion during this time of crisis again came in the form of the use of United States census data in inappropriate ways. Although the Census Bureau did not give out specific names of Japanese-Americans, it did work with the United States Government to target certain localities with high populations of Japanese people.[16] Surprisingly, this use of census data did not start in response to the attack on Pearl Harbor, instead, it began sometime in the 1930s and continued through the actual period of internment.[17] Other widespread abuses of Japanese American privacy rights occurred during this period of time, including loyalty hearings before Government officials where personal information was required to be provided and non-consensual searches of personal belongings in the internment camps.[18] The United States Government has since apologized for its widespread violation of rights during this time, but not without protest from Japanese-Americans and privacy advocates or court decisions sharply criticizing the abuse of privacy by the Government. See *Korematsu v. United States*, 584 F. Supp. 1406 (N.D. Cal. 1983). Although complete resolution of this intrusion took close to forty years, this is yet another clear example of the cycle of the imposition and lifting of invasions of privacy in response to a perceived threat to our national security.

iv. Cold War / McCarthyism

Shortly after the conclusion of World War II, tensions started to grow between the United States and the Soviet Union creating what became known as the Cold War.[19] The Cold War would last into the early 1990s, but the time of greatest concern for Americans worried about their privacy rights came during the era of McCarthyism. Named after Senator Joseph McCarthy, this movement attempted to stem the threat of communism from invading American soil.[20] The purpose of McCarthyism was to identify and criminalize communist behavior and participation in the

---

[14] Semiannual Report of the War Relocation Authority, for the period January 1 to June 30, 1946, not dated; Papers of Dillon S. Myer, available at http://www.trumanlibrary.org/whistlestop/study_collections/japanese_internment/documents/index.php?pagenumber=4&documentid=62&documentdate=1946-00-0&collectionid=JI&nav=ok (last visited February 20, 2007).

[15] The War Relocation Authority & The Incarceration of Japanese Americans During World War II, available at http://www.trumanlibrary.org/whistlestop/study_collections/japanese_internment/1941.htm (last visited February 20, 2007).

[16] *See* The Census and Privacy, *supra* note 14.

[17] *Id.*

[18] Burton M. Farrell, F. Lord and R. Lord, Confinement and Ethnicity: An Overview of World War II Japanese American Relocation Sites, c. 16 available at http:///www.cr.nps.gov/history/online_books/anthropology74/ce16.htm (last visited February 20, 2007).

[19] *See* William M. Wiecek, The Legal Foundations of Domestic Anticommunism: The Background of Dennis v. United States, 2001 Sup. Ct. Rev. 375, 406-423 (2002).

[20] Even though the movement was named after McCarthy, its scope was not limited to just the Senator's actions. The term McCarthyism will be used to describe not only events after Senator Joseph McCarthy became a large proponent of the movement, but also events prior to his involvement that carried the same tone and purpose.

Communist Party.[21] In order to achieve such a goal, legislation passed by the United States Government greatly liberalized the investigatory process for rooting out communists. Specifically, the United States Government, and other state and local Governments created "loyalty review boards" to investigate suspected Communists by looking through personal details of their lives such as organization memberships and educational information.[22] Another major privacy concern was the fact that the Federal Bureau of Investigation was freely sharing "allegedly" confidential information garnered during loyalty reviews with various Government agencies and private companies.[23] Along with these blatant privacy intrusions, the United States Government also enacted various pieces of legislation requiring suspected Communist organizations to register with the Government and authorizing deportation of immigrants or nationalized citizens thought to be involved with subversive activities.[24]

As McCarthyism gathered momentum, opposition to it grew and public dissent became louder. Amid this growing groundswell against McCarthyism, various court decisions helped to blunt its impact. See e.g., *Slochower v. Board of Education*, 350 U.S. 551 (1956) (finding that using Fifth Amendment Privilege against self-incrimination regarding membership in the Communist Party could not impute a "sinister connotation"); *Yates v. United States*, 354 U.S. 298 (1957) (holding that believing in a forcible overthrow of the Government was not actionable without actually encouraging others to take action); *Watkins v. United States*, 354 U.S. 178 (1957) (curtailed the power of a Congressional investigation committee to punish uncooperative witnesses with unpopular beliefs); *Kent v. Dulles*, 357 U.S. 116 (1958). Once again, conforming to pattern, the perceived threat of communism prompted the Government to take invasive measures which were later withdrawn when their adverse effects were shown to have gone too far.

III. The USA Patriot Act

B. The Passage of the Act

Enacted exactly forty five days after the 9/11 terrorist attacks, the USA Patriot Act was an extensive piece of legislation aimed at enhancing national security and revamping the United States' domestic counter-intelligence capabilities.[25] Even though relatively minimal, the initial public ire directed at the passage of the USA Patriot Act stemmed largely from the fact that the act was passed with little legislative debate, yet affected a plethora of citizens' rights.[26] Surprising to some, the fact that the USA Patriot Act contained provisions that had repeatedly been rejected by Congress in years prior to 9/11 caused only

[21] To achieve this goal, Congress conducted the House Un-American Activities Committee hearings and passed such legislation as the anticommunist oath provisions of the Taft-Hartley Act of 1947, Pub. L. No. 80-101, 61 Stat. 136 (1947). and the McCarran Act of 1950, Pub. L. No. 81-831, 64 Stat. 987 (1950).

[22] President Truman's Executive Order 9835 initiated a program of loyalty reviews for federal employees in 1947.

[23] The information was shared many times with the House Un-American Activities Commission and private employers in order to coerce firings.

[24] The McCarran Internal Security Act of 1950, supra note 22; Immigration and Nationality Act of 1952, Pub. L. No. 82-414, 66 Stat. 163 (1952).

[25] *See* Douglas J. Sylvester and Sharon Lohr, Counting on Confidentiality: Legal and Statistical Approaches to Federal Privacy Law After the USA Patriot Act, 2005 Wis. L. Rev. 1033, 1057 (2005) citing Craig S. Lerner, The USA Patriot Act: Promoting the Cooperation of Foreign Intelligence, 11 Geo. Mason L. Rev. 493 (2003); Michael J. Woods, Counterintelligence and Access to Transactional Records: A Practical History of the USA Patriot Act Section 215, 1 J. Nat'l Secur. & Pol'y 37 (2005).

[26] Robert O'Harrow Jr., Six Weeks in Autumn, Wash. Post, October 27, 2002, at W06.

minimal criticism at the time of passage.[27] To compensate for the absence of a thorough legislative debate, a sunset clause, was inserted in the Act to mandate the expiration of certain provisions on December 31, 2005 if not renewed prior thereto.[28] After two extensions of this deadline[29], the USA Patriot Act was ultimately renewed[30], but not without increasing criticism of the legislation's effect on civil liberties, including the right to privacy.[31]

In reality, the USA Patriot Act was not entirely new law. Instead, it amended already existing laws relating to privacy and national security.[32] The Act was passed to ease restrictions on governmental intrusions into privacy when investigations were related to terrorism.[33] This is not to say that the intrusions have not arguably exceeded their scope throughout the years the USA Patriot Act has been in effect;[34] in fact, the historical trends also suggest that past instances of governmental intrusion initiated during times of crisis have gone beyond their original intentions.[35]

[27] Surveillance Under the USA PATRIOT Act (April 3, 2003), available at http://www.aclu.org/safefree/general/17326res20030403.html (last visited February 14, 2007).
[28] USA Patriot Act, *supra* note 2 at § 224.
[29] Congress originally passed an extension giving until February 3, 2006 to come to an agreement regarding renewal of the Act. After an inability to compromise out of a Democratic fear for abuse of civil liberties, Congress agreed to extend the deadline for renewal another five weeks until March 10, 2006. The renewal was signed into law March 9, 2006. *See* Caron Carlson, Congress Extends Patriot Act Another Five Weeks, available at http://www.eweek.com/article2/0,1895,1918597,00.asp (last visited February 23, 2007).
[30] This renewal was not a complete reauthorization of the USA Patriot Act as it was originally written. *See supra* note 5.
[31] *See* Gallup Poll, *supra* note 4.
[32] *See* USA Patriot Act, *supra* note 2 generally; Sylvester and Lohr, *supra* note 26 at 1058.
[33] Jim Cornehls, The Death of Privacy: The USA Patriot Act, 3 No. 1 Andrews Privacy Litig. Rep. 2 (September 22, 2005).
[34] *See Id*.
[35] *See* discussion *supra* Parts II(A)(i-iv).

C. Key Provisions and Their Effect on Privacy in the United States

i. Section 203 (Freer Inter-Agency Information Exchange)

Generally speaking, Section 203 of the USA Patriot Act enables Government agencies to exchange information more freely than prior to the events of 9/11.[36] By amending 18 U.S.C. § 2517, Section 203(b)(1) of the USA Patriot Act served to allow Government agencies to disclose contents of any wire, oral, or electronic communication, or evidence derived therefrom, to any other federal agency to the extent that the information pertained to foreign or counterintelligence, or assisted in the performance of the receiving agency's duties.[37] Similar to Section 203(b)(1), Section 203(d)(1) allows any foreign intelligence information obtained as part of a criminal investigation to be disclosed to any federal agency to assist the official receiving that information to perform his or her duties.[38] This section clearly blurs the line between a criminal investigation and foreign intelligence gathering, thereby creating a potential for abuse. The abuse could occur by an agency disguising a criminal investigation as intelligence gathering, in order to have the benefit of a lower legal standard applied to intelligence operations.[39] Another potential abuse is that of information warehousing.[40] The argument is that Section 203 encourages

[36] USA Patriot Act, *supra* note 2 at § 203(b) and (d). These provisions allow agencies such as the FBI, CIA and other agencies to share information without regard to how the information was obtained.
[37] *Id.* at § 203(b)(1)
[38] *Id.* at § 203(d)(1)
[39] Kate Martin, Why Sections 203 and 905 Should Be Modified, available at http://www.abanet.org/natsecurity/patriotdebates/203-2#opening (last visited February 20, 2007).
[40] *See Id.*

Government agencies to collect and keep information on as many different people for as long as possible, instead of focusing on potential terror threats, thereby sacrificing the personal privacy of the United States public at-large.[41]

It should be noted however, that this section of the USA Patriot Act does have some built- in privacy protections. Specifically, when the information, obtained through grand juries or wiretaps, pertains to a U.S. citizen, then the U.S. Attorney General must create proper procedures for the disclosure of any "foreign intelligence information."[42]

ii. Section 206 (Expanded, Target-Focused Surveillance)

Section 206 of the USA Patriot Act widens the Government's ability to use wiretapping in order to gather and monitor intelligence.[43] In order to accomplish its goal of broadening roving surveillance authority, Section 206 of the USA Patriot Act amended the Foreign Intelligence Surveillance Act of 1978 ("FISA") (namely, § 1805(c)(2)(B)). Section 206 grants broad-scale roving surveillance authority after requiring a court order approving an electronic surveillance to direct any person to furnish necessary information, facilities or technical assistance in circumstances where the Court finds that the actions of the surveillance target may have the effect of thwarting the identification of a specified person.[44] More precisely, this section allows surveillance to focus on the target, rather than the device the target is using, when attempts are being made to avoid identification of the device.[45]

Section 206's potential for invasion of privacy is great. First, by expanding the use of roving surveillance without proportionally increasing the series of checks and balances on the procedure, it largely increases the potential for abuse by federal authorities, simply by making it easier to gain access to private communications. Moreover, by lowering the standards for obtaining a wiretap, this legislation clearly enhances the chances of an innocent person's communications being intercepted.[46]

iii. Section 215 (Any "Tangible Things" Can Be Requested)

Under the USA Patriot Act, Section 215 grants the Government broad authority to seek any "tangible things" necessary for an investigation into terrorist related activity.[47] Section 215 is another section of the USA Patriot Act that effectively amends FISA. Specifically, Section 215 grants the Government authority to order "the production of any tangible things for an investigation to protect against international terrorism or clandestine intelligence activities..."[48] This section opens the door to production of many different kinds of things, whereas prior to the USA Patriot Act the Government was limited to requesting "records" only.[49] Additionally, this section also broadens the Government's ability to compel production from any business, not from just "a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility" as FISA allowed.[50]

---

[41] John T. Soma, Maury M. Nichols, Stephen D. Ryerson, Lance A. Maish and Jon David Rogers, Balance of Privacy Vs. Security: A Historical Perspective of the USA Patriot Act, 31 Rutgers Computer & Tec. L. J. 285, 310 (2005).
[42] USA Patriot Act, *supra* note 2 at § 203.
[43] *Id*. at § 206.
[44] *Id.*
[45] *Id.*
[46] James X. Dempsey, Why Section 206 Should Be Modified, available at http://www.abanet.org/natsecurity/patriotdebates/206-2#opening (last visited February 20, 2007).
[47] USA Patriot Act, *supra* note 2 at § 215.
[48] *Id.* at § 215(a)(1).
[49] Christopher Wolf, Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age, § 8-15 (2006).
[50] 50 U.S.C.A. § 1862.

This section's vagueness will likely lead to abusive invasions of privacy. By making all "tangible things" available for inspection, the Government is given free reign over what to compel for production without adding any significant checks on its power. In order to compel production under this section, the Government must be involved in an "authorized investigation" of terrorism, meaning that the entity to which the Government is requesting production from need not even be the target of investigation.[51] Clearly, this kind of broad investigatory authority could lead to widespread and abusive intrusion of privacy.

iv. Section 216 (Expanded Access to Electronic Communications)

Section 216 of the USA Patriot Act regulates the Government's access to electronic mail and other computer network traffic / electronic interception matters.[52] Section 216 effectively amended the Electronic Communications Privacy Act ("ECPA")[53] to authorize monitoring on more than just "pen registers."[54] Section 216 allows the Government to authorize installation of devices for recording all computer "dialing, routing, addressing, or signaling information."[55]

Because the original ECPA did not require probable cause to access information[56], the threat to privacy posed by Section 216 is quite clear. With this amendment to the ECPA, the Government can effectively build a file on any individual who uses the internet in any capacity, as long as the Government deems the investigation to be a criminal matter. Apart from any potentially dangerous information that can be accessed, the Government can obtain information relating to every website visited by a particular individual, ranging from personal e-mails all the way to internet shopping habits.

v. Sections 507 & 508 (Access to Educational Records and Data)

Sections 507 and 508, two of the most controversial sections of the USA Patriot Act, grant the Government access to educational data being sought in connection with a terrorism investigation.[57] Section 507 amends Section 444 of the General Education Provisions Act[58] and allows the Government access to educational records from any educational agency or institution.[59] Likewise, Section 508 amends Section 408 of the National Education Statistics Act of 1994[60]and allows the Government to gather information collected by the National Center for Educational Statistics for the investigation and prosecution of terrorism.[61]

Sections 507 and 508 allow the Government access to information that has long been held in confidence by educational institutions. The fact that the records can now be obtained with a mere court certification[62] worries many people that the United States Government has overstepped its bounds. Clearly, these Sections of the USA Patriot Act come under scrutiny not necessarily because of the actual release of documents, but instead because of what kinds of personal information the documents contain.

---

[51] USA Patriot Act, *supra* note 2 at § 215.
[52] *Id.* at § 216.
[53] Specifically, this section amended 18 U.S.C.A. § 3121(c).
[54] "Pen registers" include numbers dialed, received or otherwise transmitted via a telephone line to which a monitoring device has been attached.
[55] USA Patriot Act, *supra* note 2 at § 216(c)(2).
[56] The ECPA required only a showing that the "information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." ECPA *supra* note 54 at § 3123(a)(3).
[57] USA Patriot Act, *supra* note 2 at §§ 507-508.
[58] 20 U.S.C.A. § 1232(g)
[59] USA Patriot Act, *supra* note 2 at § 507.
[60] 20 U.S.C.A § 9007 (since repealed, but remaining in another section with only minor changes; 20 U.S.C.A. § 9573(e)).
[61] USA Patriot Act, *supra* note 2 at § 508.
[62] *Id.*

D. Other Effects of the USA Patriot Act on Privacy of U.S. Citizens

Since the passage of the USA Patriot Act, the United States Government has tracked census information regarding Arab-Americans.[63] Although this type of examination was not explicitly authorized by the Act, it appears that this monitoring would not have taken place but for powers granted to the Government under the USA Patriot Act.[64] Clearly, this is a worrisome development, even if the Government has stated its reason for requesting this data was to understand where Arabic-American signage needed to be posted in airports.[65] Even though this measure taken by the Government is a threat to citizens' privacy, it is completely consistent with the historical pattern we have demonstrated.[66]

E. Recent Legislative Developments and Case Law Affecting the Right to Privacy

The most significant legislative development since the initial passage of the USA Patriot Act was the re-passage of the Act on March 9, 2006.[67] This renewal made fourteen sections of the USA Patriot Act permanent, provided for the expiration of two of the most controversial sections of the Act, and added some new safeguards for prevention of abusive privacy intrusion.[68] Under the renewed provisions, Section 215 now requires high-level approval[69] and reporting of requests for certain records, including library, bookstore, tax return, gun sales, educational and medical records.[70] In addition to this approval and reporting requirement, the amended Section requires judicial review of requests for information under this section.[71] Further, both Sections 206 and 215 will expire altogether in 2009.[72]

Since the re-passage of the USA Patriot Act in March 2006, there have been no significant new cases decided regarding the law as amended.[73] The weakening of the Act effected by the legislative re-passage seems to have held many challengers at bay, but that is not to say that continued challenges to the USA Patriot Act have not or will not be mounted. The scant caselaw decided in response to challenges to the original Act has only minimally limited the powers granted the Government by the Act.

One notable line of cases has dealt with the Act's impact on privacy rights. In Doe v. Ashcroft ("Doe I"), the court was asked to consider whether 18 U.S.C. § 2709 as amended by Section 505 of the USA Patriot Act, which authorized the Federal Bureau of Investigation to issue National Security Letters ("NSLs") to compel internet service providers to both turn over and keep secret

---

[63] *See* Freedom of Information Documents on the Census: Department of Homeland Security Obtained Data on Arab-Americans from Census Bureau, available at http://www.epic.org/privacy/census/foia/default.html (last visited February 15, 2007).

[64] *See Id*., While true that U.S. Census data is often thought to be protected from intrusion, it is clear that the Government requested and received this type of information in response to the 9/11 attacks.

[65] Sylvester and Lohr, *supra* note 26 at 1068.

[66] *See* Discussion *infra.*

[67] USA PATRIOT Improvement and Reauthorization Act of 2005, *supra* note 5.

[68] *Id.*

[69] High-level approval must come from either the FBI Director, Deputy Director or Official-in-Charge of Intelligence. USA PATROT Improvement and Reauthorization Act of 2005, *supra* note 4 at § 215.

[70] Bush Renews Patriot Act with New Privacy Safeguards, 3 No. 8 Andrews Privacy Litig. Rep. 15 (April 18, 2006).

[71] Id.

[72] USA PATRIOT Improvement and Reauthorization Act of 2005, *supra* note 5.

[73] There have been judicial challenges to the Act as it existed prior to its re-passage; however, those challenges have been largely unsuccessful, and also fall outside the scope of this article. Any successful judicial challenges were effectively integrated into the new version of the USA Patriot Act during its re-passage.

requests for their customers activities on the internet, was proper.[74] The court found this law unconstitutional on two grounds: (1) § 2709 violated the Fourth Amendment of the U.S. Constitution because by requiring complete secrecy, the NSLs were prohibiting judicial review and thereby immunizing the NSLs from any judicial process, and; (2) § 2709 was found to be a prior restraint on protected anonymous speech and a content-based restriction on constitutionally protected speech.[75] In *Gonzales v. Doe* ("Doe II"), the court was again asked to look at § 2709 as amended by Section 505 of the USA Patriot Act to determine whether the Government could enforce a gag order placed on Doe II insofar as it restricted Doe II from informing people he was a recipient of an NSL.[76] Again, the court found § 2709 had suppressed Doe II's speech and enjoined the Government from enforcing the gag order, reasoning that § 2709 violated Doe's First Amendment rights as a content-based, prior restraint on speech.[77]

The Government of the United States filed a consolidated appeal in both of these cases, and while the appeal was pending, the USA Patriot Act re-passage took effect. In the case of Doe I, in light of the new law, the appellate court found that the Fourth Amendment ruling no longer applied because of the requirement for judicial review added during the re-passage of the Act, but remanded the First Amendment issue to the Southern District of New York to determine whether the re-passage of the USA Patriot Act had resolved that issue.[78] In the case of Doe II, because the Government decided to concede that Doe II could disclose its identity, the appellate court found that there was no basis for appeal.[79] These cases demonstrate the willingness of the Courts to restrict the powers granted to the Government by the USA Patriot Act where their exercise is perceived as an undue intrusion upon the right of privacy.

IV. Looking At The Future Of Privacy Under The USA Patriot Act Using A Historical Lens[80]

History reveals a pattern where, first, in times of crises when our national security is perceived to be threatened, the Government enacts laws and takes other measures which invade our right to privacy and other liberties and, then, when the crises passes or the impact of these measures is challenged as being unduly intrusive, those measures are rescinded or cut back either by legislation action or judicial decision. Thus, we may anticipate that the intrusions upon the right to privacy that have been permitted by the USA Patriot Act will ultimately be softened or rejected altogether when the threat of terrorism has abated, if not before.

F. The USA Patriot Act and the Alien and Sedition Acts of 1798

Like the four Alien and Sedition Acts of 1798, the USA Patriot Act permits large scale governmental intrusion into the privacy of U.S. citizens because of a perceived threat to national security. Even though the Alien and Sedition Acts of 1798 did not explicitly authorize forms of privacy intrusion, the types of measures it enacted required the Government to overstep its bounds in investigating both U.S. citizens and aliens. Like the USA Patriot Act, the Alien and Sedition Acts used the fear generated by an outside subversive group to

[74] Doe v. Ashcroft, 344 F. Supp. 2d 471 (S.D.N.Y. 2004).
[75] *Id.* at 494-526.
[76] Doe v. Gonzales, 386 F. Supp 2d 66 (D. Conn. 2005).
[77] *Id.* at 72-82.
[78] Doe I et. al. v. Gonzales, 449 F.3d 415, 419 (2d Cir. 2006).
[79] *Id*. at 420-21.
[80] The genesis of the idea for this analysis stemmed from the article by Soma et. al. *supra*, note 42. Instead of focusing on a statistical legal analysis, as the Soma article did, this article uses a historically fact-based legal analysis to examine the issue of privacy intrusion.

convince U.S. citizens of the need for enhanced security which could best be enforced through sacrificing personal privacy.

Many of the outcomes stemming from the privacy intrusions allowed by the Alien and Sedition Acts are analogous to the results of the USA Patriot Act. The Alien and Sedition Acts created stricter barriers for citizenship of aliens living in the United States.[81] Similarly, Sections 507 and 508 of the USA Patriot Act have allowed the Government to access foreign alien educational records in order to ensure that upon their visa expirations the aliens return to their home countries.[82] Further, the monitoring of anti-American writings authorized by the Alien and Sedition Acts closely mirrors some provisions of Section 216 of the USA Patriot Act which permit the monitoring of e-mail and internet transmissions.[83] This type of restraint on speech gives concern to not only Constitutional scholars but also privacy advocates because the means by which the Government retrieves this information is arguably questionable.

Much like the USA Patriot Act, overtime the Alien and Sedition Acts of 1798 provoked increasingly harsh opposition from both the U.S. public and various politicians. As has been previously noted, three fourths of the Alien and Sedition Acts were repealed by 1802 due to the public outcry[84], which culminated in the election of a new President who promised to overturn the Acts, and legislative change instituting privacy rules more in tune with the public desires.[85] Although this reaction was more rapid than the reaction which the United States is currently experiencing to the USA Patriot Act, the Alien and Sedition Acts were passed because of a potential, but never overt, threat from French Revolutionaries, whereas the USA Patriot Act was passed because of an actual attack on U.S. soil and the corresponding threat immediately after those attacks. The 9/11 attack served to increase the latitude the U.S. public gave the Government because the attack changed the threat from potential to real, but as can be seen in recent times, the deference initially shown to the Government may prove to be short-lived.

G. The USA Patriot Act and the United States Civil War

The actions taken by the United States Government during the Civil War also follows the established pattern The largest similarity between privacy intrusion during the Civil War and privacy intrusion allowed by the USA Patriot Act is the use of American census data. Although the current United States Government maintains that its use of census data is for completely innocuous purposes, the fact of the matter is that census data is not intended to be used for profiling purposes. Further, the Government has admitted to using the census data to single out Arab-Americans, and in doing so has mimicked the way in which census data was used during the Civil War. In the Civil War, the census information was used to predict where the enemy could be found.[86] Coincidentally or not, census data has been used since 9/11 to pinpoint the locations of Arab-Americans[87], the group the U.S. public most associates with terrorism in the United States. Further, the suspension of habeas corpus during the Civil War closely emulates the way in which Arab-Americans and Muslims were treated immediately following the 9/11 attacks and subsequently thereafter with assistance from the USA Patriot Act.[88]

---

[81] *See* Naturalization Act, *supra* note 7.
[82] *See* USA Patriot Act, *supra* note 2 at §§ 507-508.
[83] *See Id.* at § 216; *see also* Sedition Act, *supra* note 10.
[84] *See* Alien and Sedition Acts 1798, *supra* note 6.
[85] *Id.*
[86] *See* The Census and Privacy, *supra* note 14.
[87] *See* Freedom of Information Documents on the Census, *supra* note 64.
[88] Andrew E. Taslitz, Fortune Telling and the Fourth Amendment: Of Terrorism, Slippery Slopes, and Predicting the Future, 58 Rutgers L. Rev. 195 (Fall 2005) citing M. Cherif Bassiouni, Don't

Another similarity is that both instances of privacy intrusion happened with little or no debate.[89] The lack of debate allowed the intrusion to happen unchecked for some time and probably lead to increased scrutiny and complaint from the public in both instances.

If the Civil War is any guide, then it is safe to say that as the threat of terrorism decreases, the need for the measures authorized by the USA Patriot Act will recede. Like the response during the Civil War, the USA Patriot Act was an attempt to provide enhanced security to U.S. citizens in a time of increased threat of grave harm. In both instances, the measures taken by the Government were effective in initially calming society's' fears, but also served to intrude upon the privacy of its citizenry.

H. The USA Patriot Act and the U.S. Internment of Japanese Americans During World War II

Fueled by a direct attack on United States soil, much like the attacks of 9/11, the United States' response during World War II coincides with the type of privacy intrusion felt by the U.S. public after the passage of the USA Patriot Act. When Japanese-Americans where placed in internment camps their property and possessions were subject to inspection by the United States Government.[90] Much like Section 215 of the USA Patriot Act, where the Government can request production of any "tangible thing", the invasion of privacy in the Japanese internments camps was unabridged by any limiting law. During the Japanese internment, the U.S. Government again used national census data inappropriately to target the location of Japanese-Americans. Similarly, the USA Patriot Act has indirectly served to allow the Government to inappropriately use census information to assist in locating Arab-Americans.[91] Additionally, the use of the USA Patriot Act's provisions to root out suspected terrorists and place them in military jails at Guantanamo Bay, Cuba, is quite similar to the internment of Japanese–Americans.

Interestingly, the internment of Japanese-Americans was a product of an attack on U.S. soil. The bombing of Pearl Harbor intensified anti-Japanese sentiment in the United States and prompted the U.S. public to accept the internment as necessary for the prevention of further attacks. Ultimately, however, the internment ended, and in subsequent years, amid much public outcry, the United States District Court for the Northern District of California condemned the internment. See *Korematsu*, 584 F. Supp. 1406. It may take a similar length of time for the demise of the USA Patriot Act because of the immediacy of the continued threat of terrorism and because the images of 9/11 are still ingrained in the memories of almost every United States citizen.

I. The USA Patriot Act and the Cold War / McCarthyism

The privacy intrusion during the McCarthy era may be one of the best analogues to the intrusion sanctioned by the USA Patriot Act. During the McCarthy era, the United States Government shared information freely between agencies, whether the information involved a verifiable threat or merely a rumor regarding potential involvement in the Communist Party.[92] Similarly, Section 203 of the USA Patriot Act allows for greater information sharing between Government

---

Tread on Me: Is the War on Terror Really a War on Rights in Civil Rights in Peril: The Targeting of Arabs and Muslims, 1 (Elaine C. Hagopian ed., 2004).

[89] The Civil War's laws were enacted under Presidential Emergency powers and the USA Patriot Act was the result of piece of legislation that passed with no debate out of fear for future, imminent terrorist attacks. *See supra* note 28.

[90] *See* Farrell et. al., *supra* note 19.

[91] *See* Freedom of Information Documents on the Census, *supra* note 64.

[92] *See supra* note 24.

agencies.[93] Section 203 raises great concerns with the U.S. public given its potential for abuse and the prevailing view that some agencies should not be privy to certain information. Additionally, during McCarthyism the Government collected information by focusing on the target of the information, not on the means by which the information was collected.[94] Section 206 of the USA Patriot Act essentially allows for the same kind of behavior by the Government which could lead to large scale privacy intrusion as it did during the Cold War. Further, during the McCarthy era, the Government sought records relating to education and other various, seemingly unrelated aspects of a person's life to investigate a potential threat.[95] Sections 507 and 508 of the USA Patriot Act permit similar Government behavior.

McCarthyism also illustrates the pattern we have discerned. In response to an alleged threat of Communism, the United States Government implemented measures that were oppressive to individual privacy in the United States. Likewise, the USA Patriot Act's intrusions upon privacy were implemented out of fear of terrorism. Even though the intrusion during the era of the Cold War lasted for a fairly long time[96], it eventually succumbed to public pressure and judicial intervention.

J. How the USA Patriot Has Already Begun Following the United States Privacy Invasion Cycle

If one looks closely at recent polls and judicial scrutiny, the USA Patriot Act is slowly beginning to follow the established pattern of the cycle of privacy intrusion in the United States. As mentioned earlier, public opposition to the USA Patriot Act's intrusion into privacy is growing[97] and becoming a source for change. Further, the courts have already begun their review of questionable provisions of the USA Patriot Act, and seem willing to overturn provisions perceived as having gone too far. Lastly, the legislature itself, through re-passage of the Act in March 2006, has begun its review of the Act and has already taken corrective measures to protect the privacy of United States citizens.

After reviewing the governmental action regarding privacy rights during previous times of national fear and crisis, a pattern can be clearly seen. It is certainly more than just a coincidence that during every prior threat to national security cited in this article, the United States Government has reacted by intruding on its citizens' privacy. Further, it proves true that during every instance of wide-scale intrusion, there is a corresponding building of resentment toward the Government's intrusive action. Ultimately, through public outcry, legislative change and judicial intervention, the United States Government's privacy intrusion is scaled back to normal levels where the general public feels more comfortable with Government involvement. Clearly, this cycle of intrusion upon, and subsequent restoration of, the right to privacy has been repeated many times throughout history, and is an accurate predictor of the future of the USA Patriot Act's impact in our lives. This is the natural ebb and flow of privacy protection and intrusion in the United States. Barring a further unforeseen major terrorist attack occurring within the United States[98], the USA Patriot Act will likely continue its gradual demise and make way for the restoration of privacy rights to the degree that prevailed immediately prior to 9/11.

---

[93] USA Patriot Act, *supra* note 2 at § 203.

[94] The McCarran Internal Security Act of 1950, *supra* note 22.

[95] USA Patriot Act, *supra* note 2 at §§ 507-508.

[96] The era of true McCarthyism lasted roughly ten years, while the Cold War itself lasted for a much longer period of time into the early 1990s ending with the fall of the Soviet Union.

[97] *See* Gallup Poll, *supra* note 4

[98] Though it would not change the ultimate result, another terrorist event would likely delay the running of the U.S. Government's privacy intrusion cycle.

V. Conclusion

Many of the outspoken critics of the USA Patriot Act contend that the United States Government has clearly overstepped its bounds in enacting this law. Further, they assert that the Act impermissibly intrudes on United States citizens' privacy rights in an unprecedented and overreaching manner. To answer these critics, this article would suggest putting the USA Patriot Act into the context of the times in which we live and to remember the history the United States has endured. Was the USA Patriot Act passed without substantial review, effectively granting the US Government powers it currently did not enjoy? Yes. Did the USA Patriot Act intrude on the privacy of United States citizens in ways not allowed leading up to 9/11? Definitely. But the real question to be asked is whether the USA Patriot Act's privacy intrusion is truly greater than any similar instances of privacy intrusion in the country's history, and given that history, whether the intrusion will continue unchecked for the long-term future of the United States. The answer to that question is probably not. As Machiavelli wrote, "Whoever wishes to foresee the future must consult the past; for human events ever resemble those of preceding times. This arises from the fact that they are produced by men who ever have been, and ever shall be, animated by the same passions, and thus they necessarily have the same results."[99] Although justified in their beliefs, critics of the USA Patriot Act should realize that this Act's intrusion into privacy is merely a part of the cycle of privacy intrusion in the United States, and that barring another catastrophic terrorist event, a return to privacy equilibrium will occur.

[99] Niccoló Machiavelli, The Discourses, (1517).

The Corporate Attorney-Client Privilege: Preserving Privacy in an Age of Transparency

By: J.H. Huebert and David Douglass

I. Introduction

The sanctity of the attorney-client relationship is one of the oldest legally respected private relationships, in the form of the attorney-client communication privilege.[1] Indeed, it even predates the common law. Under Roman law, a lawyer's loyalty to his client forbade him from being a witness against the client. As the concept evolved under English common law, the rationale changed, becoming more grounded in the client's right to preserve his secrets; a right to privacy.[2] This concept logically embraced the communications a litigant would necessarily engage in with counsel representing his or her interests in legal proceedings. The legal profession has long appreciated that the assistance of legal professionals to represent the interests of parties would be of little value if the system required the lawyer to reveal the interests his or her client was seeking to protect. As the Supreme Court recognized in the late nineteenth century: "If a person cannot consult his legal adviser without being liable to have the interview made public the next day by an examination enforced by the courts, the law would be little short of despotic. It would be a prohibition upon professional advice and assistance."[3]

Like virtually any public policy, the attorney-client privilege entails trade-offs. After all, it deprives litigants, and derivatively society, of highly relevant evidence, possibly including evidence of crimes. Against the benefits described above – the right to legal representation, encouraging consultation with counsel to avoid committing crimes in the future – one must weigh the costs, which include allowing those who have caused harm to avoid paying compensation, or allowing the guilty to go unpunished.

The attorney-client privilege has long been extended to corporations as well as individuals,[4] but their nature presents numerous questions concerning the scope and application of the privilege, with which

J.H. Huebert is a litigation associate at Porter Wright Morris & Arthur in Columbus, Ohio. Before joining Porter Wright, he earned his juris doctor from the University of Chicago Law School, and then served for one year as a law clerk to Judge Deborah Cook of the United States Court of Appeals for the Sixth Circuit.

David Douglass is a partner in the Washington, D.C. office of Shook, Hardy & Bacon where he practices in the area of corporate criminal defense and other government enforcement actions, especially on behalf of pharmaceutical and medical device manufacturers. David is a graduate of Harvard Law School and Yale College.

[1] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (citing 8 J. Wigmore, Evidence § 2290 (McNaughton rev. 1961) ("The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law.").

[2] *See* Lance Cole, Revoking Our Privileges: Federal Law Enforcement's Multi-Front Assault on the Attorney-Client Privilege (And Why It Is Misguided), 48 VILL. L. REV. 469, 474-80 (2003).

[3] *Id.* (quoting Connecticut Mut. Life Ins. Co. v. Schaefer, 94 U.S. 457, 458 (1876)).

[4] *See* Upjohn, 449 U.S. at 390 (United States v. Louisville & Nashville R. Co., 236 U.S. 318, 336 (1915)).

the courts have long struggled.[5] In recent years, the privilege as extended to corporations[6] has come under increasing attack from the U.S. Department of Justice and in the courts. Critics argue that the costs of the privilege, constraining the truth-seeking aspect of the legal process, have come to outweigh its benefits, a concern driven by the belief that the privilege has been used improperly to shield unfavorable facts from exposure.[7] One commentator has noted that many courts around the country assume that corporations are especially prone to abusing the privilege by "funneling" documents through legal counsel, particularly in-house counsel, leading these courts to impose a heavier burden on corporations in establishing privilege than they do on individuals.[8]

While the two sides of this debate tend to invoke extreme examples, the reality for most businesses is that the issues they confront concerning the applicability, use, scope and loss of the attorney-client privilege are much more nuanced and complex, which can render proper and effective use of the privilege challenging. This challenge is heightened by changing law, the way corporations function, and the fact that the concept of the attorney client privilege has become so ingrained and ubiquitous that it fosters among corporate executives, employees, and even lawyers a conventional wisdom about the privilege's scope and applicability that is too frequently misguided.

This article examines the nature and applicability of the corporate attorney-client privilege generally, its limits, and current threats against it, and considers how corporations can exercise the privilege in a manner that is non-abusive and most effectively preserves privacy in an age of transparency. Although it focuses on these issues in the context of litigating with the government, especially criminal matters, the observations are generally applicable to private party litigation.

II. The Corporate Attorney Client Communication Privilege

A. Elements of the Privilege

The attorney-client privilege protects communications from a client to his attorney. To establish the privilege, a party must show (1) a communication, (2) made between privileged persons, (3) in confidence, (4) for the purpose of seeking, obtaining, or providing legal counsel.[9] Technically, the privilege applies only to communications from the client to the attorney, not the reverse. Still, as a practical matter, communications from the attorney to the client are protected to the extent that disclosure would effectively reveal the client-to-attorney communication.[10]

---

[5] *See,* e.g., *Id.*; Susan W. Crump, The Attorney-Client Privilege and Other Ethical Issues in the Corporate Context Where There Is Widespread Fraud or Criminal Conduct, 45 S. TEX. L. REV. 171, 174-76 (2003).

[6] Although the focus of this article is the corporate attorney client, many of the issues apply to any business or organization, including, for example, non-profits, voluntary associations, and partnerships. *See* e.g., U.S. Sentencing Guidelines § 8A1.1 (defining an "organization" under the Organizational Sentencing Guidelines).

[7] *See,* e.g., Christine Hatfield, Comment: The Privilege Doctrines – Are They Just Another Discovery Tool Utilized by the Tobacco Industry to Conceal Damaging Information?, 16 PACE L. REV. 525 (1996).

[8] Grace M. Giesel, The Legal Requirement of the Attorney-Client Privilege: A Special Problem for In-House Counsel and Outside Attorneys Representing Corporations, 48 MERCER L. REV. 1169 (1997).

[9] *See* Colin P. Marks, Corporate Investigations, Attorney-Client Privilege, and Selective Waiver: Is a Half-Privilege Worth Having at All?, 30 SEATTLE UNIV. L.R. 155, 158 (2006) (citing Edna Selan Epstein, The Attorney-Client Privilege and Work-Product Doctrine 35 (3d ed. 1996)).

[10] *See* Steven M. Abramowitz, Note, Disclosure Under the Securities Laws: Implications for the Attorney-Client Privilege, 90 COLUM. L. REV. 456, 457 n.2 (1990) (citing, *inter alia*, MCCORMICK ON EVIDENCE § 89, at 212 (E. Cleary 3d ed. 1984)).

It is important to note that the privilege pertains only to legal advice – or communications with a mixed purpose in which the legal purpose is dominant.[11] This becomes an issue in the corporate context, because attorneys are often asked for *non-legal* advice – i.e., business advice. Thus, courts are frequently called upon to determine whether a communication between an attorney and a client is legal or non-legal. Also, the privilege does not apply to communications of facts.[12] Much litigation and much criticism regarding abuse of the privilege stems from a belief that businesses can apply the privilege label to underlying facts, especially documents, they are seeking to conceal but that simply is not so. Of course, there certainly can be a degree of game-playing in characterizing information as part of a communication and not a mere fact.

The client must have intended the communication to remain confidential and must act to preserve this status. Failure to maintain confidentiality may lead to waiver, discussed below. This is especially important for corporations because of the number of people who will receive and follow the advice.

B. The Corporate Privilege

The attorney-client privilege has been applied to communications between corporations and their attorneys at least since 1915.[13] A corporation is, of course, a legal fiction – it can only act through individuals. Thus, courts long disputed which individuals' communications with corporate counsel were privileged. Some courts applied the "control group" test, under which a communication was privileged if the employee making it was in a position to control or take a substantial part in making a decision the corporation might make on the attorney's advice.[14] Others applied the "subject matter" test, under which a communication was privileged if the employee made the communication at the direction of his superior and the subject matter was within the scope of his employment.[15]

In *Upjohn Co. v. United States*, the United States Supreme Court explicitly rejected the "control group" test, because that test does not satisfy one of the important purposes of the attorney-client privilege – open communication from clients to attorneys. The Court noted: "In the case of an the individual client the provider of the information and the person who acts on the lawyer's advice are one in the same. In the corporate context, however, it will frequently be employees beyond the control group . . . who will possess the information needed by the corporation's lawyers."[16] In place of the control group test, the Supreme Court did not establish a different clear-cut rule, but instead held that whether the privilege applies should be evaluated on a case-by-case basis.[17] The essential principle *Upjohn* establishes, however, is that communications generally will be privileged if made in confidence to the corporation's attorneys for the purpose of allowing the attorney to give the corporation legal advice.

C. Limits on the Privilege

As alluded to above, the concept of the attorney client privilege has become so ingrained that it can induce a false sense of security. The privilege is neither absolute nor irrevocable. As its name indicates, the

[11] *See Id.* at 463.
[12] Upjohn, 449 U.S. at 395.
[13] *See* Louisville & Nashville R. Co., 236 U.S. at 336.
[14] *See Id.* at 390.
[15] *See* Harper & Row Publishers, Inc. v. Decker, 423 F.2d 487, 491 (7th Cir. 1970); see also generally Bufkin Alyse King, Comment: Preserving the Attorney-Client Privilege in the Corporate Environment, 53 ALA. L. REV. 621, 625-26 (2002).
[16] Upjohn, 499 U.S. at 391.
[17] *Id.*, 499 U.S. at 396-97.

protection for the confidentiality of attorney client communications is a privilege not a right. It can be relinquished, intentionally or inadvertently, or even taken away.

1. Waiver

The privilege can be waived by failing to maintain it – that is, by disseminating communications beyond "client" and counsel. Even if only a "significant portion," but not all, of a communication is disclosed, the privilege may be considered waived as to the whole communication.[18] On the other hand, the privilege is not waived where the third party has a "common legal interest" with the disclosing party, or where the communication is disclosed by the attorney to third parties acting as his or her agents for purposes of assisting the attorney in rendering legal advice, such as experts.[19]

2. Waiver Through the Advice of Counsel Defense

The advice of counsel defense negates the intent element of a crime, the idea being that a person who sincerely sought advice on how to comply with the law could not have intended to break it. A party asserting this defense must show "(1) full disclosure of all pertinent facts to counsel, and (2) good faith reliance on counsel's advice."[20] The price for relying on this defense, however, is waiver of the attorney-client privilege.[21] Understandably, the government expects to be able to scrutinize all relevant communications, rather than just those hand-picked by a defendant.

In light of the increasingly complex and constantly evolving legal environment in which business operate, the ability to not only seek advice of counsel but also to invoke that advice as a defense to a claim of wrongdoing benefits corporations greatly. At the same time, however, the concomitant prospect of revealing the advice drastically limits the zone of privacy corporations can rely upon. Because allegations of wrongdoing can be inextricably linked to the legal advice rendered contemporaneously, disclosing privileged advice frequently becomes not a question of whether but when.

A wrinkle to the advice of counsel defense may arise where a third party relies on the advice of a corporation's counsel. There is authority for the concept of a *derivative* advice of counsel defense in situations in which where "the interests of the defendant and the person on whose counsel he is relying are substantially the same."[22] In *FEC v. Friends of Jane Harman*, Hughes Aircraft Company hosted a fundraising event for a Congressional candidate, Jane Harman. To ensure that the event complied with federal election law, Hughes Aircraft's director of public affairs consulted the company's law firm. The firm advised the public affairs director on how to conduct the event lawfully, and she in turn relayed that advice to a Harman campaign staff member, who relied on it. It turned out, however, that the procedures Hughes Aircraft followed in gathering contributions on Harman's behalf were unlawful. The FEC argued that the Harman campaign should not be allowed to avoid a penalty for the violation under the advice of counsel defense. The Court held, however, that the campaign's reliance on advice given to

---

[18] *See* Marks, *supra* note 9 at 163-64.

[19] *See Id.* at 164 (citing *Ferko v. NASCAR*, 218 F.R.D. 126, 134); *see also United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961) (Friendly, J.) (attorney's use of an accountant in client's case did not waive privilege).

[20] United States v. Lindo, 18 F.3d 353, 356 (6th Cir. 1994).

[21] See Alyssa Hall & Adam M. Schoeberlein, Securities Fraud, 37 AM. CRIM. LAW REV. 941, 981 (2000) (citing United States v. Bilzerian, 926 F.2d 1285, 1292-93 (2d Cir. 1991)).

[22] FEC v. Friends of Jane Harman, 59 F. Supp. 2d 1046, 1058 (C.D. Cal. 1999) (quoting Douglas Hawes & Thomas Sherrard, Reliance on Advice of Counsel as a Defense in Corporate and Securities Cases, 62 VA. L. REV. 1, 28 (1976)).

Hughes Aircraft demonstrated its good faith – and therefore no disgorgement or penalty was appropriate.[23]

There is a certain logic to the result in *Harman*. Upon closer consideration, however, rather than articulate a variation on the advice of counsel defense, a better reasoning would have simply been that to the extent Hughes had in fact communicated to Harman's campaign the advice it had received, it had waived the privilege, rendering the advice discoverable and admissible by Harman. Regardless, the case does exemplify the challenges of both using and protecting advice of counsel. Once an organization obtains the advice of its counsel, in most instances it can only act through the actions of others inside and outside of the corporation who may ask the reasonable question, "Is what we are doing legal?" To the extent the answer is yes, the organization risks waiver, especially where that answer is provided to non-employees. Even as to employees who may be within the scope of the corporation's privilege, however, there can be significant problems. In the event of litigation, civil or criminal, against the employee, he or she may be tempted to invoke the advice of counsel defense. Yet the privilege attendant upon this defense is not the employee's to waive. In the event the corporation declines to waive the privilege, the employee is at risk of being placed in the unenviable position of being deprived of a viable defense. Although no cases have addressed this scenario, it is one that confronts prosecutors and defense counsel, for both the corporation and the employee. To the extent that an employee is entitled to assert an advice of counsel defense against a valid threat of prosecution, a rule that the employee may disclose, i.e., waive, what he or she was advised with respect to the conduct at issue seems appropriate. Under what circumstances and to what extent corporate officers, employees and third-parties who act in reliance on advice of counsel can force a waiver of the privileged communications remains to be seen. In the meantime, employers should beware.

[23] *Id.* at 1058-59.

3. The Crime-Fraud Exception

The crime-fraud exception is another increasingly common challenge in civil and criminal litigation, particularly in grand jury investigations. Courts consider the privilege waived with respect to any attorney-client communications made in furtherance of, or to conceal, ongoing or future criminal or fraudulent conduct. Generally, a party seeking to defeat the privilege through the crime-fraud exception must show that the client's communications to counsel pertained to crimes presently occurring, or which the client intended to commit in the future.[24]

The government bears no heightened burden in asserting the exception; there is no presumption in favor of the privilege. To the contrary, the government need only show a "factual basis adequate to support a good faith belief by a reasonable person . . . that *in camera* review of the materials may reveal evidence to establish the claim that the crime-fraud exception applies." If the government does so, the court conducts an *in camera* review to determine whether exception applies.[25]

The party whose privilege the government seeks to overcome need not be given an opportunity to rebut the government's prima facie case, nor does that party even have a right to know what the government's basis is for claiming the exception applies. Some commentators have decried this unfairness but courts frequently do provide the target of the investigation an opportunity to

[24] *See* H. Lowell Brown, The Crime-Fraud Exception to the Attorney-Client Privilege in the Context of Corporate Counseling, 87 KY. L.J. 1191, 1219 (1998/1999).

[25] United States v. Zolin, 491 U.S. 554, 570-71 (1989).

respond.[26] In practice, even assuming the government obtains court approval to obtain privileged information, the producing party will likely have an opportunity to seek judicial relief prior to production, for example through a motion to quash. Given the interests most companies have in defending the privilege, the better practice is for the government to notify the company and afford it an opportunity to have a judicial hearing.

When considering the crime-fraud exception, is it is a common error to place the emphasis on "crime" ignoring the "fraud" prong. This is a significant mistake because fraud embraces a much broader ranger of conduct than crime. And, of course, many things can be characterized as possibly reflecting plans to commit a *future* fraud. Characterizing conduct as fraudulent eases the government's burden in invoking this exception to obtain privileged information Even if the court determines, upon *in camera* review, that the exception does not apply, the judge will have already seen the material in question, which compromises privacy and may result in prejudice against the target despite the judge's best intentions.

4. Inadvertent Disclosure and Electronic Communications

C. Inadvertent Disclosure

The widespread use of electronic communications, email and document sharing, multiplies the risk and likelihood that communications intended to be privileged will be disseminated to people outside the scope of the attorney-client relationship. Many individuals, including individuals outside of a corporation, may be copied on e-mails, and replies may be wittingly or unwittingly sent to individuals never intended to see them. Even if senders and recipients of e-mails exercise the utmost care, preserving the documents' privacy and privilege during the discovery process may be prohibitively costly. The majority view is that inadvertent disclosure of privileged material results in waiver of the privilege with respect to the disclosed documents, but not necessarily in discovery where large numbers of documents are produced.[27] As one court has noted, where thousands or even millions of electronic documents may be produced, to require "record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation."[28]

Waiver, however, is the intentional relinquishment of a known right. Thus, a truly inadvertent disclosure should not result in waiver. In many cases, however, disclosures that are labeled inadvertent were not inadvertent at all. Rather, in such cases disclosure of the documents was intended but the disclosing party did not realize they contained privileged information and when that information is revealed, the disclosing party seeks to avoid a broader subject matter waiver. In a common scenario in which thousands, and indeed sometimes millions, of documents are disclosed when some of them contained privileged communications, the question arises: was the disclosure intentional or inadvertent? Certainly, the producing party intended to disclose the documents. The more pertinent question is whether it intended to disclose privileged communications contained within those documents, or whether the disclosure was truly inadvertent. The

[26] *See* Brown, *supra* note 24, at 1261-62. The author's experience has been that courts often provide an opportunity to respond and argue why the privilege should apply.

[27] *See* Brian M. Smith, Note, Be Careful How You Use It Or You May Lose It: A Modern Look at Corporate Attorney-Client Privilege and the Ease of Waiver in Various Circuits, 75 U. DET. MERCY L. REV. 389, 400 (1998).

[28] Hopson v. City of Baltimore, 232 F.R.D. 228, 224 (D. Md. 2005).

answer will of course turn on the facts.[29] Thus, businesses should take great care in how they choose to produce documents in discovery, to avoid unintended disclosure of privileged communications and also to create a record that any disclosure was truly inadvertent, i.e., that whatever was disclosed slipped through the cracks. Frequently, litigants will complain about the expense and burden of rigorous privilege review – giving rise to the question of how much it is worth to preserve the privilege. It is not entirely unreasonable for society to place such a premium on fact finding that it attaches a high cost to the disclosure of privileged information; this does not preclude litigants from making a cost-benefit analysis as to how much of their resources should be devoted to preventing disclosure. On the other hand, society also has a tremendous interest in expeditious and cost-effective dispute resolution, which weighs in favor of non-waiver.

Proposed Federal Rule of Evidence 502 seeks to balance these competing interests. It provides that inadvertent disclosure of privileged material (or protected work product) "does not operate as a waiver in a state or federal proceeding if the disclosure is inadvertent and is made in connection with federal litigation or federal administrative proceedings – and if the holder of the privilege or work product protection took reasonable precautions to prevent disclosure and took reasonably prompt measures, once the holder knew or should have known of the disclosure, to rectify the error, including (if applicable) following the procedures in Fed. R. Civ. P. 26(b)(5)(B)."

This new rule has laudable intentions, but it may not be very helpful at preserving privacy. As an initial matter, it is questionable whether a rule of evidence is the appropriate vehicle for achieving these results at all. The Rules of Evidence generally govern *admissibility*, not discoverability. Limiting the effect of a scope of waiver beyond its evidentiary impact is more a matter for the rules of procedure, civil and criminal. It is difficult to see how the rules of evidence can govern discoverability between and/or among the parties to litigation as well as with third parties.

Further, an inadvertent disclosure could prompt the recipient or another who becomes aware of it to seek discovery based on that disclosure. The inadvertently disclosed piece of evidence will not be admissible, but other evidence that would not have been discovered but for the inadvertent disclosure will serve the same purpose. Or, the inadvertent disclosure could alert the opposing party that the crime-fraud exception may apply. In any event, once privileged information is inadvertently disclosed, it is well and good for the Rules of Evidence to say that the privilege is not waived, but in fact the cat is out of the bag – even if the inadvertently disclosed item is not admissible, it has made others aware of the facts contained or alluded to in that privileged item. Privacy is thus lost, and the ostensible purpose of the privilege – encouraging open attorney-client communication – is not well served.

D. Selective Waiver

Related to inadvertent disclosure is selective waiver, disclosing privileged information to certain parties most commonly the government, while preserving it as to others, such as private litigants. With the exception of the Eighth Circuit Court of Appeals, the appellate courts have rejected the notion of "selective

[29] *See*, e.g., Transamerica Computer Co. v. IBM Corp., 573 F.2d 646, 652 (4th Cir. 1978) (privilege not waived because party had been compelled to produce 17 million pages of documents in three months and took reasonable precautions); *New* Bank of New England v. Marine Midland Realty Corp., 138 F.R.D. 479, 480-84 (E.D. Va. 1991) (party took insufficient precautions to avoid disclosure and therefore waived the privilege).

waiver."[30] The dominant view appears to be that endorsed by the Third, Fourth, and D.C. Circuits, under which disclosure of confidential information to a third party effects a general waiver of the attorney-client privilege for that information with respect to the entire world.[31] The Eighth Circuit, however, has taken the view that disclosure to a third party only waives the privilege with respect to that party.[32] This approach of course encourages cooperation with government.

Is it fair for corporations to have their cake and eat it, too, by asserting the privilege selectively? The selective waiver concept benefits companies because it facilitates dispute resolution, especially criminal investigations, by reducing the prospect of opening the floodgates to private litigation based upon disclosure to the government. The government tends to favor the concept for the same reasons. On the other hand, the doctrine is criticized because it can deprive other allegedly injured parties of information that can be material to proving their claims. From a public policy perspective there are competing values; the desire to resolve disputes versus the disfavor in which obstacles to the truth seeking aspects of the litigations are viewed. The courts, with the exception of the Eighth Circuit, have struck the balance in favor of disclosure. A corporation must choose between complete confidentiality or complete disclosure.

[30] *See* Kenneth S. Broun & Daniel J. Capra, Getting Control of Waiver of Privilege in the Federal Courts, 58 S.C. L. REV. 211, 216 (2006).

[31] *See* Westinghouse v. Republic of the Philippines, 951 F.2d 1414 (3d Cir. 1991); *In re* Martin Marietta Corp., 856 F.2d 619 (4th Cir. 1988); Permian Corp. v. United States, 665 F.2d 1214 (D.C. Cir. 1981); S*ee* also on waiver generally, Brian M. Smith, Note, Be Careful How You Use It Or You May Lose It: A Modern Look at Corporate Attorney-Client Privilege and the Ease of Waiver in Various Circuits, 75 U. DET. MERCY L. REV. 389 (1998).

[32] *See* Diversified Indus., Inc. v. Meredith, 572 F.2d 596 (8th Cir. 1977).

III. The Government's Assault on the Corporate Privilege

Prosecutors, as well as civil litigants, have long expressed frustration and downright hostility to practices lawyers use to ensure the broadest protection of the attorney-client privilege, such as having one lawyer represent multiple parties, for example a corporation and its employees (sometimes extending to past and future employees) or, where that is not feasible, joint-defense agreements, which allow multiple counsel representing different parties to share information without waiving the privilege. These long-simmering frustrations erupted in the wake of the Enron-type corporate scandals causing the Department of Justice to mount a frontal assault on the corporate attorney client privilege.

A. The Thompson Memo

The Justice Department's most recent assault on the attorney-client privilege came in the infamous "Thompson Memo," a memorandum issued by Deputy Attorney General Larry Thompson on January 20, 2003.[33] That memo listed nine factors prosecutors should consider in determining whether to bring charges, and in negotiating plea agreements, including the corporation's "willingness to cooperate in the investigation of its agents, including, if necessary, the waiver of corporate attorney-client and work product protection." The memo advised that waivers should be sought in "appropriate circumstances," but did not spell out precisely the circumstances under which waiver is appropriate; it did state, however, that the waiver need generally only be with respect to "the factual internal investigation and any contemporaneous advice given to the corporation concerning the conduct at issue," but not with respect to the

[33] As of this writing, the Thompson Memo is available online at http://www.usdoj.gov/dag/cftf/corporate_guidelines.htm.

government's criminal investigation itself, except under "unusual circumstances."[34]

The Thompson Memo was the subject of widespread criticism from an unusual spectrum of critics including the ACLU, the Chamber of Commerce, the American Bar Association, and even Congress. As some commentators have noted, the waiver of attorney-client privilege under such circumstances essentially "deputizes" corporate lawyers, as the government receives the fruits of the private attorneys' investigations at the corporation's expense. The corporation's employees also pay the price, as the new material available to the government allows it to pursue them individually – even if the corporation managed to get itself off the hook.

B. The McNulty Memo

The Justice Department recently retreated somewhat from the aggressive policy of the Thompson Memo in a memorandum issued by Deputy Attorney General Paul J. McNulty on December 12, 2006 (the "McNulty Memorandum").[35] That memo acknowledged the important purpose of the attorney-client privilege and added that waiver is not a prerequisite to finding that a corporation had cooperated with an investigation. The McNulty Memorandum states that prosecutors may request waiver of the attorney-client privilege or work-product protections only where there is a "legitimate need for the privileged information to fulfill their law enforcement obligations." Whether there is a legitimate need depends upon:

(1) the likelihood and degree to which the privileged information will benefit the government's investigation;

(2) whether the information sought can be obtained in a timely and complete fashion by using alternative means that do not require waiver;

(3) the completeness of the voluntary disclosure already provided; and

(4) the collateral consequences to a corporation of a waiver.

Further, even where legitimate need exists, "prosecutors should seek the least intrusive waiver necessary to conduct a complete and thorough investigation, and should follow a step-by-step approach to requesting information."

The "step-by-step" approach articulated in the McNulty Memorandum entails first seeking what the memo calls "Category I" information – "purely factual information" such as "key documents, witness statements, or purely factual interview memoranda regarding the underlying misconduct, organization charts created by company counsel, factual chronologies, factual summaries, or reports (or portions thereof) containing investigative facts documented by counsel." Before seeking a waiver for Category I information, a prosecutor must obtain written authorization from the U.S. Attorney, who must consult with the Assistant Attorney General from the Criminal Division before granting the request.

If the Category I Information does not provide the government with enough information "to conduct a thorough investigation," prosecutors can then request a waiver for Category II information: attorney-client communications or non-factual attorney work-product. To seek Category II information, the prosecutor must have authorization from the Deputy Attorney General. The memo advises that such information "should only be sought in rare circumstances." If a corporation refuses to grant a Category II waiver, the

[34] *Id.*

[35] As of this writing, the McNulty Memo is available online at http://www.usdoj.gov/dag/speech/2006/mcnulty_memo.pdf.

government cannot hold this against it in a decision whether to prosecute.

It remains unclear just how much the McNulty Memo will constrain prosecutors. It explicitly creates no rights for corporations being investigated, and it still allows prosecutors to dig and dig for dirt until they determine that a "complete and thorough investigation" has been conducted. And while the government supposedly cannot hold a refusal to waive with respect to Category II information against a defendant, it seems naïve to believe that a corporation's decision not to waive will have no impact on an individual prosecutor's view of the company's cooperation.

IV. Preserving the Privilege in an Age of Transparency

A. Using the Privilege Sparingly

As we have seen, the long-standing attorney-client privilege serves purposes that are crucial to a just adversarial legal system. The privilege is especially critical where individuals or corporations become the target of government investigation or prosecution, because the state wields unmatched coercive power, including the power to deprive one of life and liberty.

Still, although the privilege should be inviolate, the reality is that there is pressure to compromise the privilege – and a perception exists, rightly or wrongly, that corporations in particular abuse the privilege, by "funneling" documents and information through counsel, and asserting the privilege too broadly and too often. The more corporations are perceived as abusing the privilege in these ways, the less inclined courts or anyone else will be to maintain a strong corporate privilege. Accordingly, corporations should use the privilege sparingly, to protect genuinely privileged material. Put another way, the more corporations respect the privilege, the more likely it is that others will respect it also.

B. Dealing With the Reality of Disclosure

The assumption by many companies, and their counsel, that privileged communications will remain forever confidential can foster a lack of precision as to how attorney client communications are conducted. The recognition that it may serve the client's broader legal interests to disclose legal advice it received to rebut an allegation of intentional misfeasance counsels clients and lawyers to treat all communications as if they might eventually be revealed. How a client and its lawyer discuss legal issues may greatly affect a prosecutor's, or a jury's view, as to the true nature of a transaction. This consideration assumes added force given the ubiquity of electronic communications and record keeping. E-mail facilitates rapid, extensive, productive communication, but also makes it easier to send ill-considered, intemperate or incorrect emails. To make matters worse, these communications are preserved. And, as anyone who has ever been confused by whether an email was intended to be humorous, sarcastic or hostile knows, emails lack the other cues, such as inflection or body language, necessary to ensuring that the message is understood as intended. The email sent in jest can later be construed as knowledge of guilt.

The widespread dissemination of privileged communications fits awkwardly with the intimacy implicit in the privacy concept that underpins the attorney client privileged. Thus, the business advantage can easily become a legal risk area. Recognizing that organizations act through numerous individuals does not eliminate the tension. It may be prudent to *assume* that privileged communications will ultimately be disclosed. Care should be taken to ensure that the communications are precise, considered and their confidentiality safeguarded. How will the communication appear to third-parties? What will it appear the client and lawyer were trying to do? Was the lawyer helping a client comply

with or evade the law? In a time in which lawyers feel the competitive pressure to tell the client what it wants to hear and to do so quickly, there is a great temptation to dash off a quick answer. This pressure should be resisted. The quick, incomplete answer may be damaging, and even damning.

Prudence counsels that attorney client communications should be disseminated on a need to know basis. Business executives should resist the temptation to pass along the advice to colleagues or employees who do not meet that test. Once the appropriate decision maker receives the go ahead from counsel, he or she need not forward the advice to those who will execute the transaction. They can simply be told to proceed. If the legality conduct is questioned, the decision-maker should confer with counsel to determine whether it is necessary to disclose the advice. It may be appropriate for the attorney to communicate the advice directly to the employee, assuming there is no conflict of interest. This approach should allow the employee to invoke an advice of counsel defense without risking waiver of the corporation's privilege. For example, in the *Harman* case, discussed, above, had the company put Congresswoman Harman in touch with its lawyers, she would have received the same advice without raising the specter of waiving the company's privilege.

Of course, once advice is received, it must be followed. The practical impediment to achieving this obvious guidance is the number of people involved in a transaction. Not all of them may know the material facts relied upon by counsel in rendering the advice. Circumstances can change yet not be communicated back to the lawyer, raising the prospect that if the transaction is subsequently investigated, the facts of the transaction diverge significantly from the facts assumed when the advice was rendered. Keeping the lawyer reasonably apprised as the transaction unfolds can help avoid this scenario.

V. Conclusion

As the courts have long recognized, the confidentiality of the attorney-client relationship is indispensable to effective legal representation. Preserving the privilege is also critical to a businesses ability to comply with the complex and fluid legal framework in which they operate. Yet the risks that attorney-client communications will be revealed is ever-present and expanding. To minimize the prospect that privileged communications will be disclosed, voluntarily or involuntarily, companies and their counsel must understand and respect the privilege's scope and applicability and take appropriate steps to safeguard it. Even in so doing, however, it is important to recognize that disclosure may occur and even privileged communications should anticipate that reality.

The Privacy Project III

Caveat Employer

By: William J. Heller and Scott S. Christie

Roger Duronio was expecting a $50,000 year-end bonus for 2001. Although he had only joined UBS Paine Webber at its New Jersey headquarters in June 1999, the company had had a good year and he felt that he had personally contributed to that success. He wasn't one of the high-flying traders who expected to be compensated lavishly, but the traders couldn't do their jobs without him. Mr. Duronio was a system administrator for Paine Webber. He kept the company's computer network running at peak efficiency under the most trying of circumstances. In the financial industry, annual bonuses in the hundreds of thousands of dollars were common. He just wanted the appropriate recognition for his hard work. He felt that he deserved $50,000. Company management felt differently, awarding him a bonus of only $32,500. This perceived slight set in motion a series of events that ended up costing Paine Webber over $3 million.

Mr. Duronio vowed revenge against Paine Weber. He decided to strike back at the company in a place where he knew it was extremely vulnerable: its computer system. During early 2002, Mr. Duronio managed to plant some malicious computer code, commonly referred to as a logic bomb, on approximately 1,000 of the 1,500 networked computers in Paine Webber branch offices around the country. The logic bomb was designed to "detonate" and delete all the files on the hard drives of the compromised computers at 9:30 a.m. on Mondays in March, April and May 2002 unless countermanded by Mr. Duronio. To add insult to injury, Mr. Duronio then began shorting the stock of UBS, A.G., Paine Webber's parent company, betting that the destruction wrought by the logic bomb and associated adverse publicity would cause the stock price to plummet.

The logic bomb detonated as planned on March 4, 2002 at about 9:30 a.m., the start of the financial trading day. When Paine Webber employees attempted to access their computer files, they found there was nothing to access. Chaos ensued, and Paine Webber began the slow and arduous process of assessing the scope of and remediating the harm caused by Mr. Duronio. The only saving grace was that the logic bomb had no perceptible effect on the stock of UBS, A.G., causing Mr. Duronio to lose the $21,000 he had invested in shorting that stock. After a several week trial, Mr. Duronio was convicted of planting and detonating the logic bomb and, on December 13, 2006, was sentenced to a term of imprisonment of 97 months and ordered to pay $3.1 million in restitution to Paine Webber.

The Duronio case is but one example of the larger reality that corporate computer systems and the private information contained on those systems is vulnerable to unauthorized access, destruction and theft. It demonstrates that one committed individual with inside knowledge can cause millions of dollars in damage and potential legal liability to a company. Furthermore,

William J. Heller and Scott S. Christie are partners of the law firm McCarter & English, LLP in the Newark, NJ office. Mr. Heller leads the Intellectual Property practice group of the firm. Mr. Christie formerly headed the Computer Hacking and Intellectual Property section of the U.S. Attorney's Office in New Jersey. In addition to data privacy, Messrs. Heller and Christie regularly provide counseling on network security issues, conduct internal investigations of network intrusions, and litigate copyright, trademark, and patent infringement and trade secret theft cases, particularly those with a focus on information technology.

this case serves as a reminder that a system of checks and balances within a company must extend to control over its computer system. Companies that fail to segregate the system administration function and the network security function into the job responsibilities of two or more people, for example, risk being victimized like Paine Webber, or worse.

The field of data and network security is broad. It also encompasses issues of disaster recovery and backup systems, and their separate (and equal) security concerns. These concerns take on increasing importance for those companies that outsource disaster recovery. Related to these concerns is the integration of the company's information technology department as part of a comprehensive privacy program. Finally, and often over-looked, privacy, data security and network security are close allies in the protection of a company's intellectual property.

Given the breadth of the field, the legal framework addressing data and network security is diverse. There are relevant legal protections and prohibitions to be found in federal, state and common law.

Federal Legal Obligations

In this survey, space does not allow for the detailed treatment of the sector-specific federal laws that address privacy and data security. The primary sector-specific laws are:

- The Privacy Act of 1974, 5 U.S.C. § 552a;
- The Gramm-Leach-Bliley Act of 1999 ("GLBA"), 15 U.S.C. § 6801, *et seq.*;
- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 264 & 1320d-4(b);
- The Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g;
- The Federal Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, *et seq.*;
- The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), 15 U.S.C. § 1681w; and
- The Right to Financial Privacy Act of 1978 ("RFPA"), 12 U.S.C. § 3401, *et seq.*;

These federal laws contain broad definitions that sweep many companies within their coverage. By way of example only, the definition of "financial institution" in GLBA encompasses certain employers whose business has nothing to do with financial services.

All of the issues raised by these federal statutes, though important, are outside the scope of this article. Accordingly, consultation with counsel is a necessity to determine if these laws apply and, if so, the requirements to meet the legal obligations as part of a comprehensive privacy and data security program.

Privacy in the context of data security has received the most attention from the steady and escalating progression of thefts of personally identifiable information of employees and customers. This epidemic reached the national consciousness in February 2005 with the announcement by data broker ChoicePoint that thieves posing as legitimate businesses including collection agencies made use of dozens of fraudulent accounts to run background checks on and gather the personal data of approximately 145,000 individuals.

The problem is now a full-blown crisis. On May 22, 2006, the Department of Veterans Affairs ("VA") announced that a laptop computer stolen from the Maryland residence of a VA data analyst contained personal data of all the approximately 26.5 million American veterans who were discharged since 1975 including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses. Subsequent investigation revealed that this laptop computer also stored personal data from as many as 1.1

million active-duty personnel from all of the armed forces, approximately 80% of all active-duty members, along with personal data from approximately 430,000 members of the National Guard and approximately 645,000 members of the Reserves.

Since then, hardly a week has passed without a new revelation of a breach of personal data security by a credit card issuer or processor, bank, credit union, hospital, government agency, university or online merchant. The most recent breach of security that received widespread attention in the press was the January 18, 2007 announcement by TJX, the operator of retail chains T.J. Maxx, Marshalls, Home Goods and A.J. Wright, that intruders had gained unauthorized wireless access to computer systems that handle credit card, debit card and check transactions. It wasn't until March 28, 2007 that TJX revealed some extent of the breach: at least 45.7 million credit and debit card numbers stolen over an 18 month period. The TJX data security breach has the dubious distinction of being the most pervasive, besting the previous record of 40 million compromised credit card numbers. There is even insider speculation that the full extent of the theft could amount to 200 million purloined credit and debit card numbers over a four year period.

Despite the introduction of a number of bills addressing data security in Congress during 2006, none succeeded in achieving the status of law by the end of that term. This effort has started anew with the 110th Congress by California Senator Dianne Feinstein who, on January 10, 2007, reintroduced The Notification of Risk to Personal Data Act (S. 239) which would preempt state laws to impose a uniform federal standard governing corporate obligations to notify individuals who had been victimized through a breach of security of their personally identifiable information. This bill has been followed in close succession by the Personal Data Privacy and Security Act (S. 495), the Data Accountability and Trust Act (H.R. 958), and the Cyber-Security Enhancement and Consumer Data Protection Act (H.R. 836). In light of the outcry raised by the TJX data breach, chances are good that a federal data privacy breach law will be promulgated this congressional term. Until and unless that happens, personal data security legislation remains confined to the realm of state law.

State Legal Obligations

California pioneered the legislative effort with the Security Breach Notification Act, Cal. Civ. Code §§ 1798.80 et seq., which went into effect on July 1, 2003. New York (N.Y. Gen. Bus. Law § 899-aa) and over thirty other states have followed suit and promulgated their own personal data security legislation. In general, all these state personal data security statutes identify the covered agencies, entities and individuals, specify the measure of personal data protected, define what constitutes a breach of security mandating notification, dictate the scope and timing of the obligation to notify, delineate the appropriate forms of consumer notification, explain the ability of law enforcement to delay notification to consumers, and set forth the enforcement mechanisms to address violations.

The California and New York statutes, which are very similar, typify existing state legislation in the area of data privacy breaches. These statues are broadly-worded to apply to any person or business that "conducts business" within the state and owns or licenses electronic data that contains personal information. Personally identifiable information protected by these statutes is defined as a combination of two data elements including an item of rudimentary identification information about an individual, typically first name or first initial and last name, coupled with an identifying number uniquely linked to this individual such as (a) social security number; (b) driver's license number; (c) non-driver identification card number; or (d) account number, credit or debit card

number, in combination with any required security code, access code, or password that would permit access to the individual's financial account.

Pursuant to these two statutes, a security breach occurs whenever there is unauthorized acquisition of personally identifiable information in electronic form that is unencrypted. Such an event imposes a burden upon the company to notify all affected individuals who are state residents of the data security breach "in the most expedient time possible and without unreasonable delay." A determination by a law enforcement agency that victim notification would impede a criminal investigation constitutes good cause for delaying such notification. The New York statute further imposes an affirmative obligation on the company to notify the state attorney general, consumer protection board, and office of cyber security and critical infrastructure coordination before notification may be made to individual victims.

Notification to individuals may be accomplished by (a) written notice; (b) electronic notice with the prior consent of an individual and a contemporaneous log entry; (c) telephonic notice with a contemporaneous log entry [New York only]; or (d) if the cost of notice will exceed $250,000 or the number of individuals to be notified exceed 500,000, substitute notice in the form of electronic notice to a known e-mail address, conspicuous posting on the company's website and notification to major statewide media. In California, a statutory violation potentially subjects a company to a private civil cause of action for damages and injunctive relief by any affected individual. Increasingly common is the use of class action lawsuits representing the interests of hundreds or thousands of victims of a particular data security breach. New York, on the other hand, provides no private right of action; that statute only empowers the state attorney general to bring a civil action against the company seeking damages and consequential financial losses on behalf of victimized state residents.

By virtue of the current legislative regime, a company that suffers a breach of security of personal data not only must investigate the source of the breach, determine the extent of the harm resulting from the breach, and mitigate that harm, but also must, to the extent possible, identify the state of residence of each of the potentially thousands of individual victims of that breach in order to determine and comply with its legal obligations toward the resident victims of each such state. Especially where the number of victims is large and the geographic locations of these victims diverse, such a requirement can be draconian.

Obligation Governs Destruction As Well As Preservation

A company's legal obligation to protect against the unauthorized dissemination of personally identifiable information extends beyond securing such data in its possession to include destruction of such data. The FACT Act directed the Federal Trade Commission ("FTC") to promulgate regulations designed to protect the personally identifiable information of consumers during the process of disposal. These regulations, codified at 16 C.F.R. § 682, have come to be popularly known as the Disposal Rule. Although this provision is directly applicable only to consumer reports and the personally identifiable information derived from consumer reports, the FTC encourages companies to adhere to the Disposal Rule when disposing of any personally identifiable information. Indeed, the Disposal Rule has become one of the primary objective standards for determining whether companies have been negligent in dispossessing themselves of personally identifiable information.

In a nutshell, the Disposal Rule mandates disposal practices that are reasonable and appropriate to prevent unauthorized access to or use of information in a consumer

report. By way of example, such reasonable measures could include establishing and complying with policies to (a) burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed; (b) destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; or (c) conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Such an exercise of due diligence might include (a) reviewing an independent audit of a disposal company's operations and/or its compliance with the Rule; (b) obtaining information about the disposal company from several references; (c) requiring that the disposal company be certified by a recognized trade association; and (d) reviewing and evaluating the disposal company's information security policies or procedures. Companies should embrace the Disposal Rule as a minimum standard when destroying records containing personally identifiable information.

A handful of state laws has provided more guidance in this area as exemplified by the New York law governing disposal of records containing personally identifiable information, N.Y. Gen. Bus. Law § 399-h. This New York law directly applies to any business record containing personally identifiable information which is defined in a manner broader than that contained in the New York data privacy breach statue: an item of personal information, typically first name or first initial and last name or a unique identifying number (such as a credit card number), coupled with an identifying number or code uniquely linked to this individual such as (a) social security number; (b) driver's license number; (c) non-driver identification card number; or (d) mother's maiden name, financial services account number or code, savings or checking account number or code, debit card number or code, or automated teller machine number and code.

To properly dispose of records containing personally identifiable information, a New York business must (a) shred the record before disposal; (b) destroy the personally identifying information contained in the record; (c) modify the record to make the personally identifiable information unreadable; or (d) take actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personally identifiable information contained in the record. Any violation of this New York data disposal law subjects a business to civil injunctive action by the state attorney general and a civil penalty of up to $5,000 per incident of improper disposal, even absent a showing that any individual was injured or damaged.

Common Law Obligations

Separate and apart from relying upon statutory obligations, creative counsel already have begun to argue the applicability of traditional breach of contract, real property, and tort laws to data breach cases.

It might be argued that a data breach is also a breach of contract. Dealings with an employer, with a government administration (like the Department of Veteran's Affairs), or with a third party (as in a credit card transaction) easily can give rise to a claim that the contract, either expressly or by implication, includes a covenant – an agreement or a binding contractual obligation – to receive and maintain the privacy and confidentiality of personally identifiable data.

Real property long has addressed the obligations of property owners to third parties entering on their land or into their premises. Generally, under real property law, a property owner's obligations decreases to a minimum in the case of a trespasser, and increases in the case of "business invitees." A "business invitee" is

nothing more than a person who ventures into a retail establishment to make a purchase. The mere act of being open for business and allowing customers onto the retail premises is the "invitation" to conduct business. Under the law of most states, real property owners owe an obligation of due care to business invitees.

It would not be outside the realm of aggressive advocacy for a victim of identity theft to allege that the business invitee rule imposes liability upon a store owner that had lost or mishandled personally identifiable information. This is not entirely unusual, as lawyers for several years have applied other traditional real property concepts to the Internet. For example, "trespassing" is argued to occur when one business enters onto the virtual property of its competitor – the competitor's website – and copies the data for its own use. See, e.g., *Oyster Software, Inc. v. Forms Processing, Inc.*, 2001 WL 1736382, at *12-*13 (N.D.Cal., Dec. 6, 2001).

Finally, traditional negligence principles already have formed the basis of suits alleging privacy breaches. In the current business climate, in which the media contains daily reports of data breaches by the government and business, victims of identity theft allege that businesses and others acquiring personally identifiable information have a duty to maintain the privacy and confidentiality of that data, and that the failure to exercise due care is a breach of that duty, which leads to the foreseeable and potentially disastrous result of identity theft. See, e.g., *Kuhn v. Capital One Financial Corp.*, 2006 WL 3007931 (Mass.App.Ct., Oct. 23, 2006).

The negligence cases are a concern because there is no single standard to which a business can look to determine if it is exercising due care with personally identifiable information. The Federal Trade Commission ("FTC") has announced guidelines and best practices in the form of a relatively new publication entitled *Protecting Personal Information: A Guide for Business* (www.ftc.gov/infosecurity/). However, even these guidelines are somewhat vague, and their application may differ depending on the size of the business and the nature and quantity of personally identifiable information it acquires, uses or stores in the ordinary course of its business. Another objective benchmark for judging the reasonableness of business conduct with regard to data privacy is the Payment Card Industry (PCI) Data Security Standard (www.pcisecuritystandards.org/tech/pci_dss.htm), a comprehensive set of requirements for enhancing payment account data security developed by the major credit card companies for use by merchants accepting their cards.

Indeed, common law standards even may be implied from state laws governing data security (see above). More state laws that might be used as evidence of evolving common law standards are on the horizon. In this evolving field of potential common law liability, ignoring privacy and data security programs is no longer an option.

The Employment Relationship

Firms providing metrics in the network security field estimate that employees commit the overwhelming majority of network security breaches. Employees have access to and use personally identifiable information every day, and additional steps are available to protect that data through the employment relationship.

The Federal Computer Fraud and Abuse Act

One such avenue of protection is the federal Computer Fraud and Abuse Act (the "CFAA"), 18 U.S.C. § 1030. The CFAA is primarily a criminal statute that provides the basis for federal prosecution of a panoply of computer crimes including theft of electronic data, computer fraud, computer extortion and computer hacking. This statute also allows for a private right of civil action by victimized individuals who allege and can prove economic damages.

In the employment context, the CFAA has recently been interpreted in a manner affording employers a means of pursuing disloyal employees who alter or destroy company computer data. In *Int'l Airport Centers v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Court of Appeals for the Seventh Circuit overruled a trial court dismissal of a CFAA claim brought by an employer against an employee for deleting confidential information on a company-owned laptop computer. The court ruled that by deciding to leave the company to go into business for himself in violation of his employment agreement, an employee breaches his duty of loyalty to his employer thereby terminating the agency relationship and rendering unauthorized under the CFAA his access of the company-owned laptop for the purpose of deleting company data. See also *Forge Industrial Staffing v. De La Fuente*, 2006 WL 2982139 (N.D. Ill., Oct. 16, 2006)(same).

State Criminal and Civil Statutes Governing Computer Access

Protection of electronic data in the employment context also may be accomplished through reliance upon state statute. New Jersey, like many states, provides options both in the civil and criminal realms. An aggrieved party has a sustainable cause of action in civil court against any individual who engages in (a) the knowing and unauthorized alteration, damage, theft or destruction of computer data; and (b) the knowing accessing and reckless altering, damaging, destroying or obtaining of any data or database. NJSA 2A:38A-3. On the criminal side, it is illegal to knowingly and without authorization, or in excess of authorization, (a) access any data or database; (b) alter, damage or destroy any data or database; (c) access or attempt to access any data or database for the purpose of executing a scheme to defraud; (d) obtain, take copy or use any data, database or personal identifying information stored in a computer; or (e) access and recklessly alter, damage or destroy any data or database. NJSA 2C:20-25.

The Employment Relationship Generally

Few think of the employment relationship as the first line in a quality privacy protection program. Yet existing employment processes – beginning with hiring and ending with the exit interview – already provide the tools to ramp up data and network security.

In depth background checks are now available on the Internet, and commercial investigation companies offer these checks for a fee. IT professionals should be vetted well in advance of an offer to join the company; this background check should include references from prior employers and clients. But the background check should not be limited to IT professionals, because any employee with access to personally identifiable information should encounter the same due diligence before the employment offer is extended.

In many areas of employment law, "notice" to the employee is the essential element in enforcing policies and procedures. The offer letter is the first place to start. There is no reason why notice of the companies privacy protection program should not be a prominent part of the offer letter, which the new employee should counter-sign as evidence that he or she received the notice.

The first days of employment are filled with training, the completion of forms and computer training on company systems. Those processes likewise can be the forum for reinforcing in greater detail the privacy protection program, and in communicating the employees obligations with respect to personally identifiable information. A company's privacy policies and procedures should be part of the Employee Handbook issued to each employee.

The periodic review (especially for probationary employees) is another existing tool for reinforcing obligations to maintain

personally identifiable information private. Employees are rated on many criteria pertinent to the business, and adherence to privacy policies, as well as an annual discussion of the companies' policies, reinforces the message.

Companies should consider technology as a means to control the use or dissemination of personally identifiable information used in the ordinary course of business. For example, network software exists to restrict the size of files transmitted outside the company's firewall without prior authorization. As another example, those who use laptops or personal digital assistants (PDAs) should have those devices configured with password protection for access. Moreover, the data on laptops should be encrypted to avoid the potential losses that can occur when personally identifiable information is present on lost or stolen laptops.

Dealing with Consultants or Vendors

Companies have less control over outside consultants or vendors. Unlike employees, consultants are professionals who, as a general rule, perform their services with little to no oversight by and control over their work by the employer. To maintain the proper separation, therefore, companies using independent contractors have less control than for regular full time employees – and more risk from a data security standpoint.

Independent contractors can and should be required to sign a contract. The contract should contain the same data security provisions, policies and procedures that the company's regular employees must follow.

HIPAA provides another mechanism, an agreement called the "Business Associate Agreement." Under HIPAA, contractors having access to protected and private health information are required to sign a Business Associate Agreement, memorializing their agreement to abide by company policies on protecting protected health data and the procedures they must follow. Companies should borrow the concept of the HIPAA Business Associate Agreement for both HIPAA and non-HIPAA privacy protection – giving the astute company a uniform means to address data security with outside vendors.

Outside vendors in the information technology field – whether outsourced information technology departments, data backup vendors, disaster recovery and hot site vendors, and programmers – present additional challenges. For those having access to a company's live network, unique log-ins over a secure virtual private network ("VPN") or its equivalent is only the first step. Network administrators who are separate and apart from these vendors should install and use audit or tracking software to monitor access, activity, and data transmission to and from the network – and the logs should be reviewed periodically by someone outside of the IT chain of command.

Yet another challenge with outsourced information system services arises when companies backup their data at vendor-controlled data centers. Questions of data security include: the physical location of the facility; whether the building itself is constructed to withstand a disaster; how the facility is accessed; whether the access is recorded; and where the failover sites are located if the primary data storage network is down (some may be in remote states, or even off-shore.) Finally, companies often overlook a most simple issue: what happens to the data when the outsourced or vendor relationship ends? Only sufficient contractual obligations, with third party verification, can reduce the risk of data breaches.

One other important tool to promote data security – both with vendors and regular employees – involves hiring a qualified and certified "ethical hacking" vendor to test and identify computer network vulnerabilities before rogue employee, vendors or third parties breach the company's firewall and gain unauthorized access to personally identifiable

information. An ethical hacker will be able to customize the probe to the individual network and provide a written report specifying not only its vulnerabilities, but also suggestions to strengthen its integrity. Moreover, if the ethical hacker is retained through the company's outside legal counsel, communications related to the probe and the report itself may be encompassed within the attorney-client privilege and thereby protected from compelled disclosure by a third party.

The Bottom Line of Data Security

Data insecurity is everywhere. Every business must give serious consideration to complying with an increasing array of federal and state statutes that impose potential criminal and civil liability, and to reduce the risk of a lawsuit under traditional legal theories from contract, real property and tort law. Not a week passes without news of a fresh data breach occurring even to the most careful institutions.

There is no panacea – no magic bullet – to assure any company that its data security efforts are sufficient. The effort starts with a review of business processes to identify where personally identifiable information enters, is used in, is stored in, or leaves the company, including its destruction after use. Qualified counsel should be part of the evaluation, the definition of a data security policy, and its implementation in order to seek protection under the attorney-client privilege and other applicable privileges.

Procedures should be put in place to address a data breach before it occurs, to allow a smooth reporting structure that not only will allow compliance with state data breach laws, but also will preserve the company’s good will if it is a victim of data theft or data loss. Finally, periodic reviews of these procedures at all levels and in all departments of the company, as well as the latest legal developments, will provide evidence of due diligence that reduces the risk of liability.

There is some anecdotal evidence to suggest a growing trend of criminally-inclined individuals increasingly seeking employment in jobs through which they will have access to personally identifiable information solely for the purpose of stealing that information. Is your company up to the task of meeting this as well as future unknown challenges in data privacy protection?

The Privacy Project III

Employer Surveillance of Employee Computer Use

By: Cathy Havener Greer and Rob Hunter

"Every breath you take
Every move you make
Every bond you break
Every step you take
I'll be watching you."

"Every single day
Every word you say
Every game you play
Every night you stay
I'll be watching you."
The Police

An employee in the first decade of the 21st Century could have reason to believe that the lyrics to the song by The Police are an apt description of the current state of employer-employee relations in many workplaces. According to the 2005 Electronic Monitoring and Surveillance Survey from the American Management Association (AMA) and The ePolicy Institute, employers are using computer monitoring to assess productivity, monitor workplace computer use and protect resources, including attempts to manage and avoid potential liability. The 2005 survey reports that employers' primary concern is inappropriate web surfing by employees, with 76% of responding employers monitoring workers' website connections and 65% of companies using software to block an employee's ability to connect to inappropriate websites. A number of the respondents reported firing employees for misusing the internet or for e-mail misuse.[1]

The legal issues raised by employer monitoring of employee computer use in the workplace is complex. Constitutional and common law considerations of privacy,

[1] http://www.amanet.org/press/amanews/ems05.htm

Cathy Havener Greer has practiced law since 1976. After serving as Assistant Attorney General for the State of Colorado and as Assistant Prosecuting Attorney in Missouri, she entered private practice in 1987. Her practice includes commercial litigation, the defense of businesses, public entities and officials in federal and state trial and appellate courts, mediations and arbitrations and before administrative agencies. A portion of her practice involves dispute resolution, advising companies and governmental officials, and conducting training on management and employment issues. Ms. Greer served as a member of the Executive Committee of the IADC from 2001 to 2004 and as a faculty member at its 1998 Trial Academy. She served as Chair of the IADC's Employment Committee and the Governmental Liability Committee of The Defense Research Institute.

Robert D. Hunter received his Doctor of Law degree from Cornell University after graduating from Mississippi State. In 1976, he came to Birmingham, Ala. and the law firm of Lange, Simpson, Robinson & Somerville, where he used both his engineering and legal backgrounds to defend manufacturers in product liability litigation around the country. Mr. Hunter practiced at Lange Simpson for 23 years before accepting the position of General Counsel for Altec, Inc., and its subsidiaries. Mr. Hunter has been an active member of the IADC since 1995, most recently has served as Vice President of Corporate on the IADC Board of Directors since 2004 and became the new President-Elect of the IADC in July, 2007. He is the first corporate counsel to hold the position in recent history of the IADC.

often described in abstract and theoretical terms, may collide with a company's concern for its corporate network security, employee productivity, and avoidance of liability for misuse of computer resources.

An analysis of two United States Supreme Court decisions addressing privacy generally and in the employer-employee context is illuminating as a back drop for a thoughtful consideration of privacy in the context of electronic computer monitoring in the workplace.[2] In *Georgia v. Randolph*, 126 S.Ct. 1515 (2006), Chief Justice Roberts in dissent, joined by Justice Scalia stated, "The 4th Amendment protects privacy. If an individual shares information, papers, or *places* with another, he assumes the risk that the other person will in turn share access to that information or those papers or *places* with the government." *Id*. at 1531. (emphasis in original) The case involved the propriety of a warrantless search of a marital residence based on the wife's consent and the express refusal to consent by the defendant husband. Justice Roberts' discussions of the implications of sharing information, papers, or places with another provides a basis for considering how the Court might analyze employers' surveillance of employee computer use.

Justice Roberts challenged the majority's use of a privacy analysis when,

> the very predicate giving rise to the question in cases of shared information, papers, containers, or places is that privacy has been shared with another. Our common social expectations may well be that the other person will not, in turn, share what we have shared with them with another-including the police-but that is the risk we take in sharing. If two friends share a locker and one keeps contraband inside, he might trust that his friend will not let others look inside. But by sharing private space, privacy has 'already been frustrated' with respect to the locker mate. *United States v. Jacobsen*, 466 U.S. 109, 117, 104 Supreme Court 1652 80LEd 2nd 85 (1984). If two roommates share a computer and one keeps pirated software on a shared drive, he might assume that his roommate will not inform the government. But that person has given up his privacy with respect to his roommate by saving the software on their shared computer.
>
> A wide variety of often subtle social conventions may shape expectations about how we act when another shares with us what is otherwise private, and those conventions go by a variety of labels-courtesy, good manners, custom, protocol, even honor among thieves. The Constitution, however, protects not these but privacy and once privacy has been shared, the shared information, documents, or places remain private only at the discretion of the confidant.
>
> *Id*. at 1533.

This insight into Justice Roberts' and Justice Scalia's thinking about privacy may be a predictor of their positions on issues concerning employer monitoring of employee computer use if such a case were to reach the Supreme Court.

One of the first United States Supreme Court decisions to address the extent of an employee's privacy interest in the workplace was *O'Connor v. Ortega*, 107 S.Ct. 1492 (1987). The case involved a physician and psychiatrist who worked at Napa State Hospital for 17 years until his dismissal. Before the dismissal, the Executive Director of the hospital became concerned about possible improprieties and Dr. Ortega's management of the residency

[2]Employer's "surveillance" of employees is an imprecise term that can cover wide ranging activities. This article does not address many types of surveillance that exist and may be used by some employers, i.e. biometric identification, retinal scans, facial scans, fingerprints, Global Positioning Systems (GPS), telephone monitoring, tape recording, video surveillance, drug testing or the old fashioned search of traditional paper records.

program, including whether the acquisition of an Apple II computer for use in the residency program may have been misrepresented as a donation when in fact the computer purchase was financed by possibly coerced contributions of residents. Dr. Ortega was placed on administrative leave during the course of the investigation and while on leave, a hospital administrator entered Dr. Ortega's office and conducted a search. Dr. Ortega alleged that the search of his office violated the 4th Amendment and the Supreme Court, in a plurality decision authored by Justice O'Connor, held

> that public employer intrusion on the constitutionally protected privacy interests of government employees for non-investigatory work related purposes, as well as for investigation of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable: 'determining the reasonableness of any search involves a two fold inquiry: first, one must consider "whether the... action was justified at its inception," citations omitted; second, one must determine whether the search as actually conducted "was reasonably related in scope to the circumstances which justified the interference in the first place,
>
> *Id*. at 1501 (internal citations omitted).

The Court's decision discussed at length the boundaries of a workplace context and whether offices, desks, file cabinets, closed luggage, handbags or brief cases, as well as the contents of those items are appropriate for a workplace search. Justice O'Connor wrote that

> ordinarily, a search of an employee's office by a supervisor will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct or that the search is necessary for a non-investigatory work-related purpose such as to retrieve a needed file.
>
> *Id*. at 1502

The cases of *Georgia v. Randolph* and *O'Connor v. Ortega* shed some light on the considerations that Supreme Court Justices may give to issues of computer monitoring by employers, not to mention other types of workplace surveillance. Because both cases involve constitutional issues concerning the application of the 4th Amendment to government action, they do not clarify all of the issues that will face private employers who choose to monitor their employees' computer activities in the workplace. For those private employers, an examination of the two primary Federal statutes addressing privacy issues surrounding digital information in the workplace is instructive.

Title I of the Electric Communications Privacy Act, (ECPA) makes it illegal for any person to: 1) intentionally intercept any wire, oral, or electronic communication; or 2) intentionally disclose or use the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection. 18 U.S.C. § 2511(1).

Wire and oral communications are generally self-explanatory, but a critical issue is what is meant by "electronic communication." Courts across the country are divided as to whether electronic communication includes e-mails. The 1st Circuit in *United States v. Councilmen*, 418 F.3rd 67 (1st Cir. 2005) took a broad view of "electronic communication" to include "transient electronic storage that had been to the communication process for such communication." 418 F.3rd at 85. By

including electronically stored information within the definition of electronic communication, the 1st Circuit overcame the technological issue concerning e-mails as communication or "stored communication." That issue relates to the fact that once received, an e-mail essentially resides on a hard drive or server and is not "in transit." A narrower interpretation of "electronic communication" excludes e-mails from the definition because, as one court said, an electronic communication cannot be intercepted when it is in "electronic storage" because only "communications" can be "intercepted." *See*, *Bohach v. The City of Reno*, 932 F.Supp 1232, 1236 (Nev. 1996).

Clearly, a thorough review of Title I of the Electronic Communications Privacy Act by counsel for employers is necessary and is essential to understand the Act's scope and to avoid liability for an illegal intercept or disclosure of electronic communications. It should come as no surprise that this Title, which was enacted in 1968 has not kept pace with the technological advances in electronic communications. That fact has contributed to interesting court decisions that demonstrate the struggles that judges have faced in applying the provisions of Title I to the modern technological world.

Title II of the Electronic Communications Privacy Act covers stored communications. That Title makes it illegal for any person to: 1) intentionally access without authorization a facility through which an electronic communication service is provided; or 2) intentionally exceed an authorization to access that facility and thereby obtain, alter or prevent an authorized wire or an electronic communication while it is in electronic storage. *See* 18 U.S.C. § 2701(A). In this Title, "electronic communication service" is defined to be "any service which provides to servers thereof the ability to send or receive wire or electronic communication." 18 U.S.C. § 2510(15). Again, a careful review of the elements of the Stored Communications Act and its exceptions is essential to avoiding civil and criminal liabilities.

The Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030, et seq. was expanded in 1996 from its original purposes to protect classified information maintained on Federal government computer to include as a "protected computer," any computer in "use in interstate or foreign commerce or communication." This Act prohibits accessing a protected computer without authorization and limits access to the scope authorized.

Because employers own the computers and servers in use in their businesses, the employer is generally authorized to review and inspect the information on its own computers. *See* 18 U.S.C. §§§ 2501, 2511 and 2701. The prudent message for an employer wanting to monitor employees' e-mails is to adopt a policy announcing that the employer will monitor the computer use by employees, put the policy in writing and circulate it to employees. Additionally, to the extent that an employer wants to limit Internet traffic, an employer should adopt a policy indicating restrictions on Internet use by employees and should circulate any such policy.

Case law interpreting an employer's authority to audit employee computer use has consistently been upheld where the employer has established a policy limiting the scope of the employees' computer activities in the workplace. *See Guest v. Leis*, 255 F.3rd 325, (6th Cir. 2001) (holding that no privacy interest existed where employer posted privacy disclaimer regarding computer files); *United States v. Thorne*, 375 F.3rd 679 (8th Cir. 2004)(reversed on other grounds) (holding that no reasonable expectation of privacy existed where employer's computer use policy stated employer audit use); *United States v. Angevine*, 281 F.3rd 1130 (10th Cir. 2002) (holding that no reasonable expectation of privacy existed where employer had expressed policy to monitor computer use).

An employer must also consider whether any state statute or common law privacy rights limit the employer's ability to

monitor information on the employer's computer. *See Leventhal v. Knapek*, 266 F.3rd 64, 73-74 (2nd Cir. 2001) (finding employee had legitimate expectation of privacy in contents of office computer and noting absence of employer policy limiting scope of privacy and computer use).

Several courts have adopted reasoning similar to that announced by Chief Justice Roberts in the *Georgia v. Randolph* case when considering claimed privacy rights in e-mails sent from an individual to third-parties. In *Culbreth v. Ingram*, 389 F.2nd 668, 675-676, (E.D.N.C. 2005) a plaintiff was unable to establish a 4th Amendment violation because a court found that he could not establish a legitimate expectation of privacy in an e-mail that he sent to a third-party. The court noted that even if a third-party had a legitimate expectation of privacy in the e-mail message, the plaintiff sender lacked standing to assert a violation of the third-party's constitutional rights. *See Minnesota v.* Olson, 495 U.S. 91, 95-96 (1990). The court further stated, "the sender of an e-mail loses his own legitimate expectation of privacy in the e-mail once it reaches the recipient's account." *Id*. at 676; *United States v. Jones*, 2005 WL2284283, at footnote 1 (11th Cir. 2005) (internal citations omitted)."

One other factor that weighs heavily on the issue of employee responsibility for preserving or destroying electronic communications in the workplace is the 2006 Amendments to the Federal Rules of Civil Procedure concerning "electronically stored information." An analysis of employer responsibilities for electronically stored information under the Federal Rules of Civil Procedure, any state's Rules of Civil Procedure or the Sarbanes-Oxley Act of 2002 and related regulations is beyond the scope of this article; however, it is incumbent upon every employer to determine the applicability of those Acts to its business practices.

The one constant in the world of electronic monitoring and surveillance is that changes in technology can be expected to outpace changes to the laws governing technology. Employers must be vigilant to understanding the technology that they use in their business, the technology that is available, and the laws governing use and access to that technology.

The Privacy Project III

Privacy of Workplace Drug Testing Procedures and Results

By: Kimberly D. Baker
Sheryl J. Willert and
Jacob M. Downs

Despite the increase in education about and employee assistance directed to the avoidance and treatment of substance abuse, employees and health care payors sustain billions of dollars in costs attributable to loss of productivity, employee injury, domestic violence and alcohol induced medical conditions. Employees who undergo drug and alcohol screening as a precedent to employment, in response to a workplace policy or while in treatment, are often requested by prospective or current employers or sovereign (tribal), state or federal agencies to consent to the release of drug and alcohol testing or treatment records. This paper addresses the privacy concerns that attach to drug and alcohol testing and treatment records in the work environment.

The following workplace scenarios illustrate the need for substance abuse information and the issues relating to use and dissemination of information:

Scenario A: A job candidate has submitted an application for employment to work as a long haul truck driver. Pursuant to the federal standards regulating interstate trucking, the candidate is required to submit to a pre-employment drug test. The candidate refuses to submit and is denied employment. The candidate attempts to seek redress arguing an invasion of privacy.[1]

Sheryl J. Willert is Managing Director of Williams Kastner and is resident in the firm's Seattle office. Her practice encompasses trial work, investigations, and counseling in all aspects of employment law for all types of businesses. In addition to her employment practice, Ms. Willert has mediated numerous cases and has tried cases involving personal injury, civil rights and contract actions. She received her BA degree with distinction from Duke University in 1975 and her JD degree from Vanderbilt University in 1978.

Kimberly D. Baker is a Member of Williams Kastner. She works with companies to resolve litigation involving injuries allegedly caused by defective products, including pharmaceutical and medical devices. She also represents manufacturers and other employers who have workplace issues relating to discrimination and wrongful termination. She is a member of the DRI Board of Directors and is an active member of the Federation for Defense and Corporate Counsel.

Jacob Downs is an associate in the Seattle office of Williams Kastner. His practice focuses on business litigation, employment law, and issues affecting the transportation industry. Jacob received his J.D., magna cum laude, from Seattle University School of Law in 2006. He is also a distinguished military graduate of Pacific Lutheran University where he received his B.A. in 1999.

Scenario B: A nurse at a clinic is suspected of diverting narcotics for personal use. She suffers from a chronic pain syndrome related to injuries sustained several years ago in a car accident. The nurse cannot perform the essential functions to provide direct patient care, but is

[1] For a further discussion on Department of Transportation Regulations that mandate testing see "HIPAA FAQ - Privacy: Drug and Alcohol Testing" available at http://www.hipaadvisory.com/action/faqs/dot.htm. The bulletin reiterates that certain transportation companies are not required to have donor authorization to obtain or disclose drug and alcohol records.

responsible for the administrative aspects of the medical services of the clinic. Her job duties place her in a position to have access to the narcotics kept under lock and key. She is requested to submit to a drug screen that turns up positive for the same pain medication that she is regularly prescribed by her physician. Her employer is uncertain about what the next steps should be to rule out the suspicions of diverting narcotics.

Scenario C: While operating a forklift, employee C backs into another employee who is pushed to the ground and injured. Pursuant to the workplace policy that mandates "drug and alcohol testing for all accidents for which reasonable suspicion exists that the employee's behavior demonstrates evidence of unsafe work behavior," the forklift driver is required to take a drug test. The results are positive for marijuana. The results are sent to the medical review officer who discusses the positive result with the driver who insists he has not used marijuana, but frequently hangs out with friends while they smoke marijuana. The medical review officer requests a confirmation of the screening test that is again positive. The test results are sent to the business, which offers the employee the option of being evaluated for substance abuse or termination. The employee declines either option and seeks a review with the employment review panel. He requests that the written drug test result not be submitted to the panel as he is concerned about further disclosure. The employee will stipulate verbally that the test was positive, but denies that he was smoking marijuana.

Each of these scenarios presents circumstances when the employer's policies dictate that a candidate or employee submit to drug testing.[2] The issues surface when

[2] As a general proposition, most cases involving employer's requirements for drug testing arise in the public sector. Many of those public sector cases allege violations of both the state and federal constitutions. The cases generally give rise to allegations of unreasonable searches and seizures and a violation of constitutional rights to privacy as opposed to arguments that there have been violations of HIPAA. *See*, e.g. Crager v. Board of Education of Knott County, Kentucky, et. al. 313 F. Supp 2d 690 (E.D. Ky. 2004) (court found that teachers, principals, traveling teachers, teacher aides, substitute teachers, school secretaries and school bus drivers held "safety sensitive" positions, had a diminished expectation of privacy, their jobs were highly regulated and there was no violation of the state or federal constitution); McCloskey v. Honolulu Police Department, 71 Hawaii 568, 799 P.2d (1990) (court found that there was no invasion of privacy when police officers were compelled to provide urine samples to determine if there has been marijuana or cocaine use because police officers were vested with the responsibility of providing safety to the public and preserving the integrity of the police department); O'Connor v. Police Com'r of Boston ,408 Mass 324, 557 N. E. 2d 1146 (1990) (court determined that even though drug testing was an invasion of privacy, the intrusion into the privacy of a police cadet was justified and diminished by virtue of cadet's agreement in writing at time of commencement of employment that he would submit to drug testing and because of the public interest in discovering and deterring drug use by police cadets, because of the risks to public safety, because of concerns about the integrity of the police department, because of concerns about the physical fitness of police cadets and because of the need for the public to maintain confidence in police officers and cadets who have a responsibility to uphold and enforce the law); and New Jersey Transit PBA Local 304 v. New Jersey Transit Corp., 151 N. N., 531, 701 A2d 1243 (1997) (court determined that although the state constitution required a finding of special need before there could be an invasion of privacy such as drug testing, there was a special need for transit authority employees because they carry firearms and work in a highly regulated, safety sensitive position).

Despite the fact that most of the cases involving drug testing arise in the public sector forum, there are also cases in which employees have challenged drug testing programs in the private sector. The results of the cases have been similar to those of the public sector. *See*, e.g. Satterfield v. Lockheed Missiles & Space Co., 617 F. Supp 1359 (D SC 1985) (court ruled that while there could be a cause of action stated for invasion of privacy if the employee could demonstrate that there had been a publication of private affairs or a wrongful intrusion into private activities, termination as a result of a positive drug test did not meet the necessary standard of "blatant and shocking

the employer must decide how the information will be used. With that as a foundation, the following discussion addresses acquisition of drug and alcohol test results and treatment records and the privacy restrictions placed on disclosure, security, use and redisclosure.

disregard of rights and serious mental or physical injury or humiliation resulting from such disregard); Slaughter v. John Elway Dodge Southwest/AutoNation, 107 P. 3d 1165 (Colorado Ct. of Appeals 2005), (court upheld summary judgment for employer in case where employee was terminated for refusal to submit to drug testing. Court ruled that employee had not demonstrated an unreasonable intrusion on the seclusion of another, unreasonable publicity given to another's private life or appropriation of another's name or likeness. Instead, court ruled that there was no constitutional right to refuse drug testing); Vargo v. National Exchange Carriers Association, Inc. et. al, 376 N.J. Super. 364 A. 2d 679 (2005) (court ruled that temporary employee who submitted to drug test as a condition for obtaining full time employment had no reasonable expectation of privacy and could not maintain an action against employer for invasion of privacy since employer had long standing policy of a drug free work place, employee was aware of the policy, employee signed the terms and conditions of employment which contained the policy and employee voluntarily submitted to the testing); Baggs v;. Eagle-Picher Industries, Inc., 957 F.2d 268 (6th Cir. 1992) (court dismissed multiple plaintiff case alleging invasion of privacy where employer conducted surprise drug tests after becoming aware of drug problems within plant. Court ruled that employees were aware that the company policy specifically stated that employees could be required to submit to drug testing upon request as a term and condition of continued employment); and Folmsbee v. Tech Tool Grinding & Supply, 417 Mass 388, 630 N.E. 2d 586 (1994) (court ruled that there was no invasion of privacy despite fact that company policy not only required drug testing but also required that employee disrobe and be visible when providing urine sample. Court found that this level of intrusion was not unconstitutional because of the strong interest in safety and guaranteeing the integrity of the urine sample). *See*, Wilkinson v. TimesMirror Corp, 215 Cal. App. 3d 1034, 264 Cal. Rptr. 194 (1989) and Baughman v. Wal-Mart Stores, Inc. 215 W. Va. 45, 592 S. E. 2d 824 (2003) which both suggest that status as an applicant as opposed to a regular employee may create less of a protectable privacy interest.

A. Federal Laws Lead the Way to Protect the Confidentiality of Substance Abuse Records

Recognizing that a certain societal stigma often attaches to the entry and completion of a drug and alcohol rehabilitation program, the federal government adopted very restrictive statutes that limit the disclosures, use of drug and alcohol test results, and information that a person is undergoing or has undergone evaluation and/or treatment for substance abuse.[3] The regulations are intended:

> to insure that an alcohol or drug abuse patient at a federally assisted alcohol or drug abuse program is not made more vulnerable by reason of the availability of his or her patient record than an individual who does not have an alcohol or drug problem or who does not seek treatment.[4]

To enforce this goal, a criminal penalty, assessed as a fine of not more than $500 for the first offense and not more than $5000 for each subsequent offense, may be imposed.[5] The federal laws entitled Health Insurance Portability and Accountability Act "HIPAA," compliment 42 C.F.R. Part 2. The HIPAA regulations, along with state statutes and laws, require a careful analysis in the work place to find answers to the following questions:

1. Can an employer request the result of a drug or alcohol test?
2. If the employer is entitled to get the results of a drug and alcohol test, what type is consent must be obtained from the employee donor?
3. If the employee is enrolled or has previously enrolled in a substance abuse recovery program pursuant to a

[3] 42 C.F.R. Part 2
[4] 42 C.F.R. § 2.3(b)(2)
[5] 42 C.F.R. § 2.4

return to work or similar agreement, what type of information can the employer receive about the employee's treatment and ability to return to work?

4. Once an appropriate consent has been received, which company employees are allowed access to the information?

5. How must the information be stored to protect confidentiality?

B. Applicability of the Federal Regulations

The Federal regulations providing privacy of substance abuse records apply to most work environments. Many of the state laws and health care privacy acts adopt the common elements contained in the federal statute. The federal regulations governing the privacy of substance abuse records apply to:

> "Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States."[6]

The breadth of the regulation is far reaching when consideration is given to the large number of drug and alcohol treatment programs that are financed, in whole or in part through monies received from the federal government. In addition, many clinics that provide services to evaluate, diagnose and provide follow-up care for substance abusers are recipients of federal funding through third party payors such as Medicaid or recipients of monies available through military benefits.[7]

The initial step is to determine whether this federal regulation applies to the records which the employer seeks. The statute defines the scope of protected information in 42 C.F.R. § 2.12 (e):

> "These regulations cover any information (including information on referral and intake) about alcohol and drug abuse patients obtained by a program, (if the program is federally assisted in any manner described in § 2.12(b). Coverage includes but is not limited to, treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, school-based programs, and private practitioners who hold themselves out as providing, and provide alcohol or drug abuse diagnosis, treatment or referral for treatment."

If the employer determines that the program that evaluated, treated or referred an employee is federally assisted, written consent is mandatory to obtain the test results and any other diagnostic or evaluative treatment limited to the purpose of the disclosure. The consent form must include the following:

(a) Required elements. A written consent to a disclosure under these regulations must include:

(1) The specific name or general designation of the program or person permitted to make the disclosure.

(2) The name or title of the individual or the name of the organization to which disclosure is to be made.

(3) The name of the patient.

(4) The purpose of the disclosure.

(5) How much and what kind of information is to be disclosed.

(6) The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under § 2.15 in lieu of the patient.

---

[6] 24 C.F.R. § 2.1

[7] 42 C.F.R. § 2.12(b)(1)-(6)

(7) The date on which the consent is signed.

(8) A statement that the consent is subject to revocation at any time except to the extent that the program or person which is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third party payer.

(9) The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given.

(10) This consent is subject to revocation at any time except to the extent that the program which is to make the disclosure has already taken action in reliance on it. If not previously revoked, the consent will terminate upon (specific date, even or condition).

(b) Sample consent form.

(c) Expired, deficient, or false consent. A disclosure may not be made on the basis of a consent which:

(1) Has expired;

(2) On its face substantially fails to conform to any of the requirements set forth in paragraph (a) of this section; or

(3) Is known to have been revoked.

1. Maintaining an Employee's Records

The intent of the statute is to minimize both the amount of information disclosed and the number and identity of the recipients. Dissemination of this information within the work environment is on an absolute "need to know" basis. Once the records are sent to the employer, the federal regulations require that:

(a) Written records which are subject to these regulations must be maintained in a secure room, locked file cabinet, safe or other similar container when not in use; and

(b) Each program shall adopt in writing procedures which regulate and control access to and use of written records which are subject to these regulations.[8]

To comply with these regulations, the records must not be maintained with any other personnel file or employee files. In addition to the restrictions on securing records, the regulations also prevent the redisclosure of the information received. 42 C.F.R. § 2.32 provides that no further disclosure of the records received may be made unless a written consent compliant with the regulations has been signed. Note that a general medical release or a subpoena are not sufficient to allow for production of these records.

2. Responding to a Request for Employee Records

Employers often receive requests for copies for employee work records. The request may be sent as part of a workers compensation process, a criminal investigation, or civil litigation. Under the federal regulations, the employer may produce substance abuse records maintained by an employer upon receipt of a signed written federally compliant consent.[9] Without such a written consent, the employer can only release the records to an individual or office, including law enforcement, in response to a specific court

[8] 42 C.F.R. § 2.16 (a), (b)

[9] 42 C.F.R. §§ 2.31-2.35

order accompanied by a subpoena.[10] It is not uncommon for law enforcement to request the records and present a subpoena. However, the court order that is necessary to allow disclosure in these criminal investigatory settings may only be issued under three circumstances that must be substantiated in the court record: [11] [12]

> 1. To protect against an existing threat to life or serious bodily injury, including suspected child abuse and neglect and verbal threats against third parties;
> 2. When necessary for an investigation or prosecution of an extremely serious crimes, such as one which directly threatens loss of life or serious bodily injury, including homicide, rape, kidnapping, armed robbery, assault with a deadly weapon;[13] or
> 3. Disclosure is in connection with litigation or an administrative proceeding in which the patient offers testimony or other evidence pertaining to the content of the confidential communications.[14]

3. Scope of Provider Disclosure

When issuing an order authorizing disclosure, a court must specifically limit disclosure to the parts of the patient's record that are essential to fulfill the objectives of the order and to those persons whose need for the information was the basis for the order.[15] The court's order must also include any other measures necessary to limit disclosure for the protection of the patient, the physician-patient relationship, and the treatment services.[16] For example, the court may order that the court record be sealed for a proceeding in which the disclosure of a patient's drug testing information was ordered.

Because of the ever increasing concern of privacy and confidentiality regarding personal medical information, these procedures and requirements for obtaining disclosure are strictly enforced.[17] As such, if an employer, as a records holder, finds itself forced to disclose drug testing results pursuant to a valid court order and subpoena, it must take careful measures to ensure that it only discloses the limited information authorized by the order.

Employers need to be aware that the health care providers involved with drug and alcohol treatment may also be limited in their disclosure of confidential information. If the provider falls with the statutory definition, the provider is required to disclose the least amount of information needed for the purpose of the request. If the request is to secure confirmation that an employee is attending treatment regularly and complying with the program, then the provider will only be allowed to state that

---

[10] 42 C.F.R. §§ 2.61-2.67

[11] The case law concerning the application of 42 C.F.R. Part 2 is sparse. *See* U.S. v. Hughes, 95 F. Supp. 2d 49, 56 (Mass. 2000) ("Little case law exists concerning the purpose and application of 42 C.F.R. § 2.65.")

[12] But cf.. United States v. Corona, 849 F.2d 562, 565 (11th Cir. 1988) (holding that despite the district court's failure to make findings in the record that the criteria of 42 C.F.R. § 2.65 were met regarding the disclosure of defendant's drug treatment records to law enforcement, such error was not reversible because a reasonable trial judge could have found that all the criteria were met).

[13] *See* United States v. Maddox, 1997 U.S. Dist. LEXIS 23782 at *9 (finding that, under 42 C.F.R. § 265, a supervised release revocation proceeding was not a "criminal investigation or prosecution," and therefore, the testimony of a drug counselor could not be compelled).

[14] 42 C.F.R. § 2.63

[15] 42 C.F.R. §§ 2.64-2.65

[16] *Id.*

[17] *See* United States v. Crawford, 199 U.S. Dist. LEXIS 23396 (holding that defendants had good cause for the disclosure of plaintiff's drug treatment records, but because the procedure outlined in 42 C.F.R. § 2.64(a) was not properly followed defendants were only entitled to disclosure of those documents in plaintiff's own possession and not those maintained at the treatment facility).

information. If the purpose of the request for records and scope of the consent is to seek an opinion on the employee's fitness for return to work, then the provider should limit the disclosure to the request and need for information.

Questions have also arisen regarding the release of medical information in the course of litigation and whether it is appropriate to discuss private health care information on an ex parte basis. Although the cases discussing this issue have not arisen in the employment context, employers would do well to adhere to the standards which have been set forth by courts in other litigation, namely, insure that if there is ex parte discussion, an appropriate HIPAA compliant protective order is in place.[18]

4. Use of Confidential Substance Abuse Information

Once the employer receives the information, the hard and fast rule is to limit both the scope and nature of the information to those that need to know. If the test results are a pre-employment screening, then only the Medical Review Officer, if one exists, and the hiring decision maker should see the results. If the records relate to treatment of an employee completed as a term of employment or a condition of return to work, then the records and/or information in the records should be limited to those managerial personnel who are involved with the employee discipline. The limited redisclosure of information likely necessitates that the human resource manager or decision maker not disclose the reason for an employee's absence from work due to substance abuse evaluation or treatment to the worker's managers or co-workers. Training all decision makers about the need to protect confidential information, both from a secured storage requirement and a need to know disclosure policy is key to preventing any potential harm to the employee from wrongful disclosure.

C. Effect of HIPAA on an Employer's Ability to Obtain Drug and Alcohol Records or Respond to a Request for Production of Such Records

Many of the restrictions contained in the federal regulations are also present in HIPAA "privacy" regulations.[19] The provisions that are unique to HIPAA and relate to these issues of disclosure in an employment setting are reviewed. This is a brief summary about HIPAA's application to substance abuse records.[20]

The initial inquiry in a HIPAA analysis is whether the statute applies to the situation being addressed. HIPAA applies to "covered entities" that are health care plans, including Medicaid, health providers (doctors, psychologists, hospitals, pharmacists, etc) who electronically transmit protected health information in connection with health insurance claims or other specified transactions, business associates of covered health plans and covered health care providers.[21] In the employment setting, these privacy regulations most commonly impact health care employers, companies who handle or make electronic payment for health care services and companies that process health care or disability benefits for which health care information is exchanged.

---

[18] See, e. g. Santaniello v. Sweet, et. al., No. 3:04CV806 (RNC) (D. Conn. January, 2007); Bayne v. Provost, 359 F. Supp.2d 234 (N. D. N.Y. 2005); Shroposhire v. Taylor, No. 06-10682, 2006 U.S.,. Dist. LEXOS 52943 (E. D. Mich. August 1, 2006); Croskey v. BMW of N. America, No. 02-73747, 2005 U. D. Dist. LEXIS 43442 (E. D. Mich., Nov. 14, 2005).

[19] Public Law 104-191; 45 C.F.R. §§ 160, 162, 164

[20] For a complete explanation of the intricacies of the privacy regulations under 42 C.F.R. Part 2 and HIPAA, see "The Confidentiality of Alcohol & Drug Abuse Patient Record Regulation and the HIPAA Privacy Rule: Implication for Alcohol & Substance Abuse Programs" available at http://www.hipaa.samhsa.gov/Part2ComparisonClearedTOC.htm.

[21] 45 C.F.R. § 160.103

The privacy statute restricts the type of information that may be disseminated without consent. The information that may not be disclosed without appropriate written consent is called "PHI"- Personal Health Information. PHI includes

> "any information (in any form) created or received by a covered health care provider or health plan (or business associate) regarding the provision of health care, payment for health care, or physical or mental condition of a specifically identified individual."[22]

Common work settings in which HIPAA applies are health clinics, hospitals or other treatment centers and/or the benefits coordinator for health or disability insurance. Other employment environments governed by the statute would be insurance companies, government agencies that provide payment for medical services and human resource, pension specialists or workers compensation specialists who electronically submit or receive PHI for payment.

When an employer needs copies of drug and alcohol treatment records, the employer can have the candidate or employee complete a modified consent form that complies with the federal regulations under 42 C.F.R. Part 2 and be compliant with both sets of regulations. The form must be modified to add a written statement that the information received cannot be redisclosed.

HIPAA also allows a written consent to be provided by the person's personal representative, including a guardian, parent or other person authorized to make medical decisions for the individual. The surrogate must include a description of the surrogate's authority to act on the consent form. For example, the surrogate may indicate that she is the personal representative for the estate of a deceased worker or is the court appointed guardian for a currently incompetent worker. These surrogate signators may come in to play if an employee is injured while working and is unable to provide written consent to obtain records from the employer. That situation might arise when the injured employee is seeking redress under worker's compensation or in civil litigation. When a consent form is signed, a copy of the signed consent form must be given to the employee or designee and the employer and provider must keep the copy for 6 years from the expiration date.

The employer must make sure that no information is provided without a valid written, signed consent form. Unlike the federal regulations, HIPAA allows a covered entity to produce PHI in response to a subpoena or discovery request if the covered entity is satisfied that reasonable efforts have been made to notify the individual that the information is being requested and/or to have an opportunity to seek a protective order. As such, an employer must ensure that:

1. The candidate or employee for whom drug and alcohol tests and treatment information is requested must sign or have a recognized signator sign a consent form compliant with the federal regulations.
2. If a subpoena is received seeking all records maintained by an employer, the records received from outside providers relating to drug and alcohol tests or treatment may not be produced in response to the subpoena if the employer falls under the federal statute. Good practice dictates that either a written consent or a court order, along with a subpoena be obtained before that drug and alcohol records are released.

[22] *Id.*

D. Risks to Employer for Failure to Comply with HIPAA Non-disclosure Requirements

1. No Private Right of Action Exists:

Congress failed to provide for a private right of action when it enacted HIPAA.[23] However, the failure on the part of the Congress to provide for a private right of action should give little or no comfort to employers if they are found to have violated the statute as a result of release of information protected by HIPAA. Why? Because the absence of a private right of action will not preclude the possibility that an employer may find his/her business in court, none-the-less, attempting to defend against a violation.

2. Office of Civil Rights and the Department of Justice Can Prosecute Criminally:

Enforcement of HIPAA has been delegated to the Department of Justice.[24] DOJ relies upon the Office of Civil Rights to investigate violations of HIPAA and to refer it cases which it believes should be further pursued and which may be worthy of prosecution. Since the inception of the statute, over 25,000 complaints have been referred to OCR for investigation.[25] Those complaints have covered allegations of impermissible release of information, allegations of lack of adequate safeguards associated with release, refusal or failure to provide copies or access to medical information, disclosure of more than is minimally necessary to satisfy an inquiry and failure to have valid authority for release of information. Of those complaints investigated, apparently, very few have resulted in action by DOJ. However, when DOJ has chosen to act, DOJ has acted pursuant to the criminal prosecution provision of HIPAA.

The HIPAA criminal provisions specifically state that there can be criminal prosecution of a person knowingly (1) uses or causes to be a unique health identifier; (2) obtains individually identifiable health information relating to an individual or (3) discloses individually identifiable health information to another person.[26] Penalties associated with violation of this provision are assessed based upon the severity of the violation and whether the violation was committed under false pretenses or whether the violation occur with an intent to use the information for commercial advantage, personal gain or malicious harm. In the case of the former, fines range from up to $50,000 and/or imprisonment up to five (5) years while the latter can result in fines up to $250,000 and imprisonment up to ten (10) years.[27]

3. Despite No Private Right of Action, Courts are Finding a Way to Permit Lawsuits:

Even though the HIPAA is clear that there is no private right of action, several courts have permitted lawsuits to proceed under common law theories. One of the primary ways in which litigation has proceeded is under the theory that the individuals who have filed the lawsuit are third party beneficiaries of the contracts between health care entities and their business partners. These lawsuits are often based on the theory that the entity where the contracts are being litigated subscribe to the concepts articulated in the *Restatement (2d) of Contracts* which essentially provides that

---

[23] 64 Fed. Reg. at 59924.

[24] 42 U.S.C. §1302d-6(2000)

[25] HIPAA Blog, "A discussion of medical privacy issues buried in political arcana", February 7, 2007 and Doreen Z., McQuarrie, J. D., L.L.M. Candidate,. "HIPAA Criminal Prosecutions: Few and Far Between" footnote 4 http://hipaablog.com.

[26] 42 U.S.C. §1320d-6(a).

[27] *See*, United States v. Gibson, No. CR04-037RSM, 2004 WL 2237858 (W. D. Wash. August, 2004); United States v. Ramirez, No. l 7:05CR00708 (S. d. Tex. August, 2005) and United States v. Ferrer, No. 06-60261 CR-COHN (S.D. Fla. Sept. 2006).

if a party is an intended beneficiary of the performance of the agreement, they may prosecute a lawsuit against the breaching party.[28] Since most contracts between covered entities and their business partners, by virtue of the privacy regulations interpreting HIPAA[29], contain a provisions about third party beneficiaries, these agreements make it very easy to successfully pursue such litigation.

In addition to actions brought pursuant to a breach of contract theory, courts have also permitted individuals to proceed on other common law theories. One such case recently initiated was *Acosta v. Byrum,et. al*[30], where the court ruled that the plaintiff could proceed under a theory of negligent infliction of emotional distress where the plaintiff alleged that a physician had allowed an employee of his office access to his password which she in turn used to obtain and disseminate medical information about the plaintiff. Other courts have found similar common law protections.[31]

4. Consumer Protection Laws and Other Health Information Statutes May be a Source of Litigation:

Employers should not lose sight of the potential that a violation of HIPAA could be considered by many courts to be a violation of the states' consumer protection statutes.

Although HIPAA is clearly not mentioned in those statutes, many of those statutes have been interpreted in such a manner that a violation of any statute constitutes a per se violation of those statutes. Additionally, many states have now enacted specific laws that prohibit the release of medical information. Failure to comply with these statutes may give rise to a private cause of action.[32]

Based on the foregoing, it is clear that despite an absence of a private right of action under HIPAA, employers may well find themselves subject to litigation for failure to take seriously the provisions of the law.

E. Application of State and Sovereign (Tribal) Codes to Disclosure of Drug and Alcohol Treatment Records and Test Results

If an employer is subject to state or tribal codes, and not seeking information from a federally regulated drug and alcohol treatment provider, then the disclosure must be compliant with the tribal codes or state statutes. Good practice would encourage the use of a written consent form that satisfies both the federal and HIPAA guidelines. These guidelines are the result of very extensive drafting and consideration of input provided by both drug and alcohol patients and providers. This distillation of efforts to protect against the unlimited disclosure of the identity and treatment provided to a substance abuser will further a similar purpose for those under tribal or state governments.

F. Other Federal Statutes Covering Drug and Alcohol Records in the Workplace

The Family and Medical Leave Act "FMLA" is only applicable to covered employers. If the employer is covered by the FMLA and has received drug and alcohol evaluation or treatment records from an employee to establish a serious

[28] Restatement (2d) Contacts, §302.
[29] Privacy Ruling at §164.506(e)(2)(ii)(A).
[30] Acosta v. Byrum, et. al., No. COA06-106 (N. C Court of Appeals, December 19, 2006).
[31] Jane Doe v. Community Health Plan-Kaiser Corp., No. 85529, 2000 N.Y. App. Div. Lexis 5498(N.J. App. Div. 3d Dept., May, 2000).
[32] *See*, e. g. the laws regarding confidentiality for the following states as a non-comprehensive example: Washington, R.C.W. 70.02.170; Maryland, Md. Ann., Health General §4-309; Arizona, A.R.S. § 12-2292; Iowa, Iowa Code §622.10; Idaho, Idaho Code §39-1392(b); and California, Cal. Civ. Code §56.10.

medical condition, the employer must maintain the confidentiality of the records.

"Records and documents relating to medical certifications, recertifications or medical histories of employees or employees' family members, created for purposed of FMLA, shall be maintained as confidential medical records in separate files/records from the usual personnel files, and if ADA is also applicable, such records shall be maintained in conformance with ADA confidentiality requirements[33] except that:

> (1) Supervisors and mangers may be informed regarding necessary restrictions on the work or duties of an employee and necessary accommodations;
>
> (2) First aid and safety personnel may be informed (when appropriate) if the employee's physical or medical condition might require emergency treatment; and
>
> (3) Government officials investigating compliance with FMLA (or other pertinent law) shall be provided information upon request."[34]

When the employer is dealing with either an FMLA or an ADA eligible employee who has authorized the release of information about drug or alcohol treatment, extra care must be taken for maintaining the records, but also for taking a moment to deliberate on which company individuals are in the " need to know" circle and what is necessary for disclosure. If an employee is required to attend treatment for substance abuse that requires a change in schedule, the supervisor or manager does not need to know the type of care that is being sought, rather only that the employer may need to provide a change is schedule.

SUMMARY

Having a uniform written consent form compliant with the federal regulations and HIPAA privacy rules that is used with all candidates and employees with facilitate the appropriately authorized release of records. Vigilant storage of records and a policy on who needs to know information contained in substance abuse records will limit the likelihood of claims for violations of the federal statute, defamation and breach of privacy under state law.

[33] *See* 29 C.F.R. § 1630.14(c)(1)
[34] 29 C.F.R. § 825.500

The Privacy Project III

Privacy, The New Black?

By: Monica Bhogal and Duncan Lamont

A plethora of decisions in the UK in late 2006 have turned the tide of privacy law and the balance has been tipped in favour of a stand-alone privacy right never previously thought to be available. In particular, the decision of the Court of Appeal in *McKennitt v Ash*[1] has significantly altered the landscape of privacy law in the UK. This landmark ruling will have significant consequences for the media not only in relation to the publication of tabloid "kiss and tell" stories but also unauthorised biographies and paparazzi photographs.

Monica Bhogal is a solicitor in the London law firm of Charles Russell LLP, specializing in Media Law. A graduate of Bristol University (LLB 1996) and with a diploma in international copyright law from the University of London (2002) she and her firm represent broadcasters, national and international magazine publishers and celebrities.

INTRODUCTION

- **Historical Position**

Unlike in some European countries such as France, where an individual's right to respect for his privacy is enshrined in statute, the UK does not have such an approach to rights of privacy.

Nevertheless, as early as 1848, the courts recognized the need to protect certain such rights. Prince Albert, the consort to Queen Victoria sent some private etchings made by him and the Queen to printers to have copies made. These etchings were kept secret at Windsor Castle and shown only to close friends. However, a sneaky workman took copies and they made their way to a Mr Strange who put them in a catalogue and sought to exhibit them. The courts provided relief against "a sordid spying into the privacy of domestic life"[2] and an injunction was granted.

However it was always recognized that the English law provided no direct remedy for various (sometimes "monstrous"[3]) invasions of privacy, such as when a Sunday tabloid published photographs of a celebrity actor in hospital following major surgery including his disjointed comments, in a world exclusive.[4]

- **European Impact**

Over the following years, the law was developed significantly by the Courts through application of the action of "breach of confidence". This has been necessary in view of the right to privacy under the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) which in turn has been incorporated into domestic UK law by virtue of the Human Rights Act (HRA) which came onto force in October 2000.

Article 8 of the ECHR, entitled "Right to Respect for Private and Family Life", provides:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic

[1] McKennitt v Ash [2006] EWCA Civ 1714.
[2] Prince Albert v Strange, (1838) 2de and sn 652.
[3] Kaye v Sport Newspapers, [1991] F.S.R. 62.
[4] Kaye v Sport Newspapers, *Ibid.*

society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

However this must be read alongside Article 10, entitled "Freedom of Expression", which states:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority or impartiality of the judiciary.

THE STORY SO FAR - DEVELOPMENTS 2004-2006

Although there is no "right to privacy" in English law, in view of the HRA and decisions of the European Court of Human Rights in Strasbourg (ECtHR), the English Courts have developed a right to sue for misuse of private information. But the application of and the balancing exercise between the Article 8 rights and Article 10 rights has not been without difficulty.

In *A v B*[5], which involved an application for an injunction by a married professional footballer to prevent publication of a story given to newspapers by two lap dancers with whom he had had consorted, various pronouncements were made by the Court of Appeal on the nature of privacy rights in this country.

Any interference with the freedom of the press, as protected by Article 10 of the ECHR, had to be justified, even where there was no public interest in the material in question being published. It was also considered important to factor into the equation when one party to a relationship wanted to disclose information (which affected the other party's Article 8 rights to confidentiality). The court attached significance to the nature of the relationship – with the special status of marriage at one end of the spectrum and one night stands at the other. The weight to be given to the extensive range of relationships which can exist makes a difference.

In 2004, the House of Lords found in favor of Naomi Campbell when she sued the Daily Mirror for publication of a photograph of her in the street, leaving a narcotics anonymous meeting, even though publication of the fact that she had a drug addiction and was receiving treatment for it, could not be regarded as private in the circumstances of that case.[6] Although the newspaper was entitled to 'set the record straight' (Campbell had gone out of her way in interviews to claim that she did not take drugs) the majority of the Lords thought the article should have been published without the pictures and that there was a reasonable expectation of privacy even in a public place (she was on the street) given the nature of the information conveyed – akin to information concerning medical treatment. Significantly, their Lordships were unanimous in confirming that there is no free-standing tort of invasion of privacy

[5] A v B Plc (Flitcroft v MGN Ltd) [2002] EWCA Civ 337.
[6] Campbell v MGN Ltd., [2004] UKHL 22.

but that the action of breach of confidence must include unjustified invasions of privacy. Lord Nichols went so far as to re-name it 'misuse of private information'.

Campbell was applied by the Court of Appeal in *Douglas v Hello!*[7]. Michael Douglas and Catherine Zeta-Jones had entered into a contract with OK! Magazine granting it exclusive rights to publish photographs of their wedding. A photographer secretly gained entry and took surreptitious photographs which were bought and published by Hello! Magazine. At first instance the court found in favor of all the claimants – the judge held that they had the right to control the commercialization of the wedding photographs which were akin to trade secrets and that the taking of the photographs had been in breach of confidence.

The Court of Appeal upheld the claim by the Douglases (applying *Campbell*: Hello! knew or ought to have known that the Douglases had a reasonable expectation that the information would remain private) and held the photos clearly portrayed aspects of the Douglases' private life, but rejected OK!'s claim which was based on the law of commercial confidence.

In considering the "private" information concerned it held that this had to be information that was "personal to the person who possessed it and that he did not intend it should be imparted to the general public". It was also recognized that there can be both rights of privacy and commercial rights in private information.

Compare this to the failed injunction claim by Sir Elton John[8] who was photographed walking from his Rolls Royce to the front gate of his home, casually dressed. Sir Elton claimed this was an unwarranted infringement of his privacy. He had not consented to the pictures being taken; they had been taken surreptitiously and they made no contribution to any debate on a matter of public interest. He relied on the decision of the ECtHR in *von Hannover* (the Princess Caroline case)[9].

This was an application for an interim injunction, not a full trial and so slightly different considerations came into play. This still involved the court having to consider firstly whether Sir Elton had a reasonable expectation of privacy in respect of the information in the photographs and, secondly, if so, whether that right to respect for his privacy outweighed the right to freedom of expression.

The Judge held he had no reasonable expectation of privacy - the photograph was not comparable to those in *Campbell* but more like Sir Elton 'popping out for some milk'. *Von Hannover* was distinguished as it involved an important element, namely harassment by the media. Furthermore, the recognized categories of private information, such as health, or sexual life were not involved. Just because the photo would be published with offensive text did not give rise to a cause of action.

EUROPE v UK

There has been a conflict between the European jurisprudence in this area of law and the UK courts' approach. This can be highlighted by 2 cases.

- **Princess Caroline**

Very shortly after the *Campbell* decision of the House of Lords, in 2004, Princess Caroline of Monaco won her case in Strasbourg[10]. This highly significant decision was to play a leading role in the UK although at the time it was suggested that firstly, as a European decision, it was not of binding authority in the UK and, secondly, it was confined to instances of harassment.

[7] Douglas v Hello (No 8) [2005] EWCA Civ 595.
[8] John v Associated Newspapers Ltd [2006] EWHC 1611 (QB).
[9] von Hannover v Germany, [2005] 40 EHRR 1.
[10] von Hannover v Germany, *Ibid.*

A series of photographs of Princess Caroline were published in Germany and in France. These showed the Princess engaged in activities of a purely private nature such as practicing sport, out walking, leaving a restaurant or on holiday.

It was held that the concept of private life extends to aspects relating to personal identity, such as a person's name or a person's picture; it includes a person's physical and psychological integrity and that Article 8 is primarily intended to ensure the development of the personality of each individual in his relations with other human beings: "there is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"." That protection extends beyond the private family circle and also includes a social dimension.

The ECtHR was influenced by the following considerations:

> Images can contain very personal or even intimate information about an individual.
>
> Photos appearing in the tabloid press are often taken in a climate of continual harassment. The context in which the photos were taken – without her knowledge or consent – and the harassment endured by many public figures in their daily lives cannot be fully disregarded.

The ECtHR said there is a fundamental distinction between reporting facts capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, (where the press exercises its vital role of watchdog) and reporting details of the private life of an individual who does not exercise official functions. The Princess did represent the royal family at certain cultural or charitable events, however, she did not exercise any function within or on behalf of the State of Monaco or one of its institutions.

The Court concluded that the decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the published photos and articles make to a debate of general interest.

- **The Wainwrights**[11]

Then in September 2006, the ECtHR in effect declared that the lack of a general tort of invasion of privacy in the UK violated Article 13 of the ECHR which requires the domestic law to provide an appropriate remedy available for breaches of Article 8.

Mrs Wainwright, accompanied by her handicapped son, Alan, attended a prison in Leeds to visit another son, Patrick, who was being held on remand. A prison order had been issued that all Patrick's visitors were to be strip-searched as he was suspected of using drugs.

On arrival, Mrs Wainwright and Alan were separated and were told if they did not agree to the search they would be denied their visit. They were not asked to sign consent forms until after searches were complete. Various breaches of procedure took place including the touching of Alan's genitals. The mother was severely distressed and Alan, who suffers from cerebral palsy, and then had a mental age of 12, suffered post-traumatic stress disorder.

The case went all the way to the House of Lords in the UK where it was held that as the HRA had come into effect after the acts complained of were committed, it did not apply. Furthermore, there was no common law tort of invasion of privacy and such a cause of action could only be created by Parliament.

The Wainwrights sought relief from the ECtHR. The Strasbourg court held that their Article 8 rights had been breached. Since the House of Lords had pronounced that there was no general tort of invasion of

[11] Wainwright v United Kingdom, Application No. 12350/04.

privacy, there was no remedy available for the interference with the Wainwrights' Article 8 rights and therefore there had been a violation of Article 13.

THE TURNING TIDE: RECENT INJUNCTIONS

- **X & Y v Persons Unknown**[12]

This case concerned a 'John Doe' injunction – i.e. granted against "persons unknown" - to prevent the further dissemination of allegations about the state of the Claimant's marriage. Various third party newspaper groups were served with a copy of the Order to notify them so that they would be aware, if approached with any relevant confidential information, this would or might be in breach of the terms of the Order.

The case provided guidance on the procedure for informing newspapers in such instances in advance of an application and on the way such applications are to be decided. In so doing, the Judge made a number of interesting observations.

The very nature of an injunction means Article 10 rights will be engaged. If competing Article 8 rights are also engaged then a balancing exercise needs to be carried out, without according automatic priority to either. *"It is no longer fashionable, as it was for a short time a few years ago, to describe Article 10 as a 'trump card'."*

Here, the information was of the kind most people would reasonably expect to be able to keep to themselves. The question arose whether the circumstances for this particular couple meant that they were entitled to less privacy or confidence than the general run of married couples.

A distinction was drawn between the concept of being in the public eye and that of being a publicity seeker (although sometimes there is an overlap).

Where there is information available in the public domain, it does not mean that the entitlement to privacy or private life generally has been waived. Close attention may need to be paid on how the information came into the public domain. Even well known people are entitled to some private life.

The Judge found that X, a model, was not a person who willingly set out for self promotion. She was under contractual obligations to give interviews from time to time but ordinary polite "chit chat" is qualitatively different from volunteering to release private information for public consumption.

The circumstances of marital breakdown or tension are generally unknowable by others without the revelation of private information. If there are public rows or recriminations in the media the situation will be rather different.

- **CC v AB**[13]

In a surprise decision for the media, an injunction was granted to a Claimant who had conducted an adulterous relationship for some months with the Defendant's wife, despite the Judge acknowledging that it was "a striking proposition that a spouse whose partner has committed adultery owes a duty of confidence to the third party adulterer".

Again, in the course of reviewing the specific facts, the Judge made some interesting comments.

It was held that where conflict arises between Convention rights, these are to be determined by "bringing to bear an "intense focus" on the facts of the individual case, rather than by purporting to create general principles of law judicially". Thereafter the ultimate balancing test in terms of proportionality is to be carried out.

What the Defendant is likely to say, to whom and the type of speech are of relevance – it was recognized that there are

[12] [2006] EWHC 2783 (QB).

[13] [2006] EWHC 3083 (QB).

different categories of "speech" to which greater or lesser importance may be attached: "political" v "vapid tittle-tattle" (in which there is no real public interest). Communication genuinely aimed at a close friend, members of the family, family doctor, counselor or social worker, or lawyers would be accorded a relatively high priority. Selling a story to the tabloids – whether for revenge, money or any other reason – was to be accorded lower priority. The injunction in this case prevented the latter while allowing the former and in so doing it is clear that there is a significant difference now between the traditional breach of confidence claims and the developing privacy law ('misuse of private information') since revealing private information to a few may bring down a breach of confidence claim but will not undermine a privacy claim.

The conduct of an intimate or sexual relationship is a matter in respect of which there is "a reasonable or legitimate expectation of privacy". Although it may be necessary to have regard to the nature of the relationship (perhaps a fleeting one night encounter will attract less protection).

Unlike in *A v B*[14], here neither of the parties to the sexual relationship wanted it to be made public. Here the specific facts (the relationship was over, the Claimant wanted to rebuild his relationship with his wife, his wife's fragile mental state) all involved the Claimant's family life, to which regard had to be given.

MCKENNITT V ASH

Loreena McKennitt, a Canadian citizen and folk singer and songwriter sued Niema Ash, once a friend and employee of hers.

In 2005 Ash published a book entitled *"Travels with Loreena McKennitt: My Life as a Friend"*. The book, amongst other things, disclosed private information about McKennitt relating to a number of matters including her personal and sexual relationships, her feelings about the death of her fiancé and the circumstances of his death, matters concerning her health and diet, matters concerning her emotional vulnerability, and details concerning a dispute between McKennitt and Ash arising out of a property purchase in 1997 which was the subject of litigation that had subsequently settled.

The claim was brought on the basis that some of this information had been disclosed in breach of confidence and in breach of McKennitt's privacy.

- **First instance**[15]

Her claim was successful at first instance before Mr Justice Eady in the High Court where she won £5,000 in damages and an injunction restraining publication of certain passages in the book.

In finding for the Claimant, Eady J felt that there was in essence a two point test in deciding whether the claim should succeed. The first was a threshold test of "reasonable expectation of privacy" and the second question was whether there was any "limiting factor" such as public domain or public interest, or indeed whether the information that was sought to be protected was simply too trivial or banal.

At first instance, what could be regarded as trivial details about someone's home, was still held to be private and protected. Eady J held that "to describe a person's home, the décor, the layout, the state of cleanliness, or how the occupiers behave inside it…..is almost as objectionable as spying into the home with a long distance lens and publishing the resulting photographs".

In reaching his conclusion, Eady J also relied upon the principles espoused in *von Hannover*. Although one of the deciding factors in the *von Hannover* case was the fact that Princess Caroline had been subject to many years of harassment by the tabloid press, in applying its principles here, the

[14] A v B Plc, *Ibid.*

[15] McKennitt v Ash [2005] EWHC 3003 (QB).

Judge held that there was no specific requirement for there to be longstanding harassment as such for there to be protection.

The public domain test was also expounded: the mere fact that personal information had entered the public domain in some way was not in itself decisive. What needed to be asked was whether the information is so generally accessible that in all the circumstances it cannot be regarded as confidential.

With reference to any defense of public interest, again the bar seemed to be raised. It was necessary to demonstrate a high degree of misbehavior on the part of the Claimant before reliance can be placed on a defense of public interest in "exposure of misconduct".

Ash appealed. In a decision handed down by the Court of Appeal in December 2006, the appeal was dismissed.

- **Court of Appeal**[16]

Various media organizations (The Times, Press Association, BBC) applied to intervene, given the importance of the case and its impact on the media's Article 10 rights. It was agreed that their submissions would be dealt with by way of the Judges' "taking note".

The Court of Appeal's decision, a ringing endorsement of Eady J's judgment in favour of McKennitt, set out the present state of the law in England:

- There is no tort of invasion of privacy in English domestic law.[17]
- In developing a right to protect private information, including implementation of Articles 8 and 10 of the ECHR, English Courts have to proceed through the tort of breach of confidence, into which the jurisprudence of Articles 8 and 10 has to be "shoehorned".[18]
- A feeling of discomfort arises from the action of breach of confidence being employed where there was no pre-existing relationship of confidence between the parties, and where the confidence arises from a defendant acquiring by unlawful or surreptitious means information he should have known he was not free to use (For example as in the *Douglas* and *Campbell* cases).
- This verbal difficulty is avoided by rechristening the tort as "misuse of private information"[19]
- Where, as in the present case, the complaint is of old fashioned breach of confidence i.e. arising out of a pre-existing relationship, rather than simply of the purloining of private information, that is to be taken into account.

In upholding the first instance decision, the Court of Appeal relied upon a number of findings of fact, and accepted facts, which it clearly felt were relevant to its decision.

Firstly, it was noted that McKennitt was "unusual amongst worldwide stars" as she very carefully guards her personal privacy. Indeed it seemed that Ash was all too aware of that, noting in the book that McKennitt guarded her privacy and reputation "with the iron safeguard of a chastity belt".

Furthermore, to the extent that McKennitt occasionally released information which "she felt comfortable with", this was done largely in connection with the charity she had founded concerning water safety and the prevention of boating accidents, following the tragic death of her fiancé in a drowning accident. To that extent, any comments made publicly by McKennitt on the subject of the death of her fiancé were on a limited basis.

The mere fact of her fame, and the limited revelations that she had chosen to make did not disentitle her to the protection of the law of confidence.

[16] McKennitt v Ash [2006] EWCA Civ 1714.
[17] Wainwright v Home Office [2004] 2 AC 406.
[18] Douglas v Hello (No 8) [2005] EWCA Civ 595.
[19] Campbell v MGN Ltd., ibid, as per Lord Nicholls of Birkenhead.

The essence of McKennitt's claim was that large parts of the book revealed personal and private details about her which she was entitled to keep private. To the extent that she had in the past released some information about herself, in a carefully controlled manner, did not mean that those aspects of her private life in their totality were no longer worthy of protection. Moreover, neither this nor her fame in itself placed her private life and business affairs in the public domain.

Ash, on the other hand, argued that some of the information was entirely inconsequential and did not have the necessary quality of confidence. She further claimed to have her own Article 10 right to tell her story. Furthermore, those aspects of the book that had been found to be untrue (largely relating to a property dispute) could not, by virtue of this fact, be protected. There can be no confidence or privacy in untruths.

It was held that in complaints of wrongful publication of private information, a two-step test applies:

> 1. Is the information private in the sense that it is in principal protected by Article 8? – "Essentially the touch stone of private life is whether in respect of the disclosed acts the person in question had a reasonable expectation of privacy".[20]
>
> 2. If so, in all the circumstances must be interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by Article 10? (The balancing exercise).

Article 8 – Was the Information Private?

The court then applied the first stage of the test. Determining whether information complained of is in fact private, may in many instances be dealt with easily.

If the content is "anodyne", imprecise or already known to the public, it cannot be protected. Interference with private life has to be of some seriousness before Article 8 becomes engaged.

The details published of McKennitt's personal and sexual relationships, health and diet, and her feelings in respect of the death of her fiancé may be considered self evidently private.

It should be noted that this case was different to recent leading cases such as *Campbell*, *Douglas* or *von Hannover* in that there was already a pre-existing relationship of confidence and so the problem of identifying the basis of a claim involving unauthorized or purloined information (where the primary focus has to be the nature of the information itself) does not arise in the same way. Although the court still has to consider the whether material obtained during the relationship is indeed confidential, the pre-existing relationship must be taken into account.

The fact that many of the matters were disclosed to Ash by virtue of her longstanding friendship with McKennitt made it far more difficult for Ash to argue that her rights should prevail. The book itself explicitly recognized that much of the material was confidential: for example Ash said that McKennitt "confided to me" and "revealed her innermost self to me".

Of those aspects complained of that may have been considered banal or anodyne (the description of McKennitt's cottage) the Court of Appeal agreed with Eady J's assessment that Article 8 requires "respect" to be given to a person's home such that even relatively trivial details would be protected.

A person's health is any event a private matter. The Judges found that it was "doubly private when information about it is imparted in the context of a relationship of confidence".

One of the most significant aspects of the judgment is the recognition of the European jurisprudence, in particular the *von Hannover* case. Whilst holding that

[20] Campbell v MGN Ltd., *Ibid*.

McKennitt did not really need to rely on *von Hannover* to prove her case, the Court of Appeal nevertheless made comments on it that were far reaching. It found that *von Hannover* extends the reach of Article 8 beyond what had previously been understood and that the English Courts should give respectful attention to it; that Article 8 jurisprudence did in this case, and will in the future shape the test of "reasonable expectation of privacy".

The argument by the media parties that *von Hannover* was decided on the basis that the Princess' privacy had been invaded by a campaign of media intrusion and press harassment, rather than the taking and publication of the specific photographs which in themselves would not otherwise have been an invasion of privacy was not accepted by the Court of Appeal. Whilst the Judgment of the European Court referred to media intrusion, the Court of Appeal did not consider that the general statements of principle are limited in that way.

Article 10 – The Balancing Exercise

Moving to the second stage of the test, the court reiterated that neither Article has precedence over the other. Where conflict arises an "intense focus" is necessary upon the comparative importance of the specific rights being claimed in individual case. The court must take into account the justifications for interfering with or restricting each right. The proportionality test must be applied to each.

On the question of whether there was any public interest in the publication of the book, Ash raised the argument of "shared experience": that the matters were her own experience as well which gave her a property in the information and her right to freedom of expression, to tell her own story, should be taken into account. She relied on *A v B*[21] where it was held that the fact that the two women involved chose to disclose their relationships, and exercise their Article 10 right, affected the footballer's right to protection. This argument was dismissed on the basis that the information complained about was not in fact her story at all but rather McKennitt's – Ash was merely a spectator and much of the content of the book would only be interest by virtue of the fact that McKennitt was the central character.

Furthermore, Ash had only obtained the information concerned by virtue of the nature of her relationship with McKennitt. This relationship was miles away from the "relationship of casual sex" between the footballer and the two women. "The footballer could not have thought that when he picked the women up they realized that they were entering into a relationship of confidence with him". The same clearly could not be said about this relationship.

The public interest defense is quite narrowly defined. Mere fame does not render a claimant a public figure and the mere fact that the public may have interest in a claimant does not necessarily mean that intrusion into their private lives is justified. If a public figure misbehaves then the public have the right to have the record put straight.

Ash claimed *A v B* (where the Court held that an individual who is a public figure, whilst entitled to have his privacy respected in appropriate circumstances, must recognize that because of his public position he must expect and accept that his actions will be more closely scrutinized by the media; even trivial facts can be of great interest to readers and a higher standard of conduct can rightly be expected by the public; he may be a role model; whether he has courted publicity or not, he may be a legitimate subject of public attention) took precedence over *von Hannover* so that McKennitt's private affairs could be exposed to the world whether she was a hypocrite or not.

The Court of Appeal found that the width of the rights in *A v B* could not be reconciled with *von Hannover*. *A v B*

[21] A v B Plc, *Ibid*.

however was distinguished as having not ruled definitively on the content and application of Article 10 and it was held not to be a binding authority on the content of Articles 8 and 10. Therefore *von Hannover* was required to provide the necessary guidance.

Even if *A v B* were to be followed, in this instance the claimant did not fall within the category of holding a position where higher standards of conduct can be rightly expected – the court felt this would fall within the preserve of headmasters and clergyman, politicians, senior civil servants, surgeons and journalists for example. Even if McKennitt could be considered an involuntary role model, she had made such efforts not to hold herself out as someone who's life is an open book that she could not rightly be classed as this. The point being made in *A v B* was that role models were at risk of having to put up with the reporting of disreputable conduct. Here there was none.

In respect of the public domain defense, the general principle is that information that is already known cannot claim the protection of private life.

However, the suggestion that information falling within a particular "zone" once revealed would mean that a person has a greatly reduced expectation of privacy in relation to any other information that fell within that zone was rejected.

The Court of Appeal specifically stated "if information is my private property, it is for me to decide how much of it should be published. The "zone" argument completely undermines that reasonable expectation of privacy".

It was also suggested that since Eady J had found that most of the book's allegations about the property dispute were untrue, there could be no claim in breach of confidence. However the issue of falsity went to the public interest defense. In a case of misuse of private information, the question is whether the information is private not whether it is true or false. The fact that it may be relevant to decide the truth or falsity of matters raised in support of an Article 10 claim does not mean, if matters are shown to be false, that the claim to misuse of private information then disappears.

As a result of the decision it is now clear that previously received wisdom that false personal information could not be protected is wrong. The correct question is not whether the information objected to is true or false, but rather whether it is private.

HRH THE PRINCE OF WALES V ASSOCIATED NEWSPAPERS LIMITED

In this case the Court of Appeal has reiterated a number of the principles set out in McKennitt thus cementing the new approach and laying the foundation for the course to be taken in the future.

The case concerned a journal (the Hong Kong journal) kept by HRH Prince Charles which contained a personal description of his participation in an event that marked the handing over of Hong Kong, including a banquet attended by the Chinese president, and described by him in a disparaging manner. He referred to the Chinese entourage as "appalling waxworks". The Mail on Sunday published extracts from the journal following a State visit to London by the Chinese president.

- **First Instance**[22]

It was held that Prince Charles had a reasonable expectation of privacy in respect of the Hong Kong journal and that he had not opened up the relevant zone of his life to public scrutiny. Furthermore, the journal made a minimal contribution to public debate and in balancing the Article 8 and Article 10 rights, disclosure was not necessary in a democratic society. (A claim for copyright infringement was also made,

[22] HRH Prince of Wales v Associated Newspapers Ltd. [2006] EWHC 522 (Ch).

which failed). On appeal the decision was upheld.

- **Court of Appeal**[23]

The Court of Appeal made clear that English law is to be developed in order to provide the protection that is recognized by Article 8. Therefore the Courts have extended the law of confidentiality beyond those involving a confidential relationship.

The legal principles are as set out by the House of Lords in *Campbell*. In particular the "more natural" description today is that the information is private (rather than confidential) and "the essence of the tort is better encapsulated now as misuse of private information".

As with McKennitt, this was not a claim for breach of privacy as an extension of the old law of breach of confidence. A well recognized relationship of confidence existed and as did an express contractual duty of confidentiality as well. The newspaper was aware that the journals were disclosed in breach of confidence.

The two step test was applied.

Article 8 – Was the information private?

Firstly the Court considered whether the content of the journals was confidential and private within the ambit of Article 8 and found that it was. The principles set out in *Douglas*[24] were upheld. This did not contradict the test in *Campbell*: whether the person in question had a reasonable expectation of privacy.

In any case, a test is not needed where the information is obviously private.

The journal set out the personal views and impressions of Prince Charles, in his own hand, seen by his staff who were under an express contractual obligation to treat it as confidential, and sent out marked personal and confidential.

Prince Charles' comments about the events (which themselves were in the public domain) were not in the public domain.

It was argued that Prince Charles, as heir to the throne, was a public figure who had controversially courted public attention and used the media to publicize the views, that the views expressed in the journal were political in nature and therefore he could have no reasonable expectation of confidentiality.

The Court of Appeal agreed with the first instance Judge that these matters did not go to the question of whether the journal was confidential, but rather to the weight to be given to them against the right of freedom of expression.

It was held that there is a distinction between the question of whether a Claimant can reasonably expect those in a confidential relationship with him to keep information confidential, and whether a Claimant can reasonably expect the media not to publish such information if the duty of confidence is breached.

Article 10 – the impact on an action for breach of confidence

The ECHR recognizes the importance of the role of the press in a democratic society. Where the published information invades an individual's right of privacy, as protected by Article 8, the Court gives careful consideration to whether the information is truly of public interest rather than interest to the public.

The Court referred to the discussion of the public interest defense in *McKennitt* emphasizing the significance of the fact that the information had been revealed within a relationship of confidence.

Furthermore, the courts' approach is that whether a publication or threatened publication involves a breach of a relationship of confidence, an interference with privacy or both, it is necessary to consider whether these matters justify the interference with the Article 10 rights that

[23] HRH Prince of Wales v Associated Newspapers Ltd. [2006] EWCA Civ 1776.
[24] Douglas v Hello, *Ibid.*

will be involved. A balance has to be struck.

Where there is no breach of a confidential relationship, the balance will usually involve weighing the nature and consequences of the breach of privacy against the public interest, if any, in the disclosure of private information.

Where the disclosure relates to information received in confidence, although there is a test of proportionality, this is a significant element. It is not enough that the information is a matter of public interest. The test to be applied is whether, in all the circumstances, it is in the public interest that the duty of confidence should be breached.

Note that the Court of Appeal endorsed the Judge's regard to the argument of the Prince's "private space" which is an aspect of his own "human autonomy and dignity": the right to be able to commit his private thoughts to writing and keep them private, particularly as he is a public figure who is subject to constant and intense media interest.

ANALYSIS AND CONCLUSIONS

It has been suggested that the *McKennitt* Judgment deals a blow to freedom of expression both in terms of the right to freely impart information but also the right of the public to receive such information. It is likely that the "kiss and tell" stories that are the staple diet for many tabloids will be at risk. The Judgment will have wider implications as well for unauthorized biographies not least as these cannot be authored by those who have previously been in some form of relationship with their subjects which impose duties of confidence without risk.

The law on privacy has been extended beyond what was previously thought to be the position and, although the *McKennitt* case specifically involved information that was obtained as a result of Ms Ash's position of trust, many aspects of the Judgment will be of wider application. The extension of the principles in *von Hannover* to instances where there is no harassment as such, can only lead to the conclusion that even a single photograph, in a public place, may be considered to be an invasion of privacy. This type of material would previously have been regarded as innocuous and anodyne enough that it could not rightly be regarded as having the necessary quality of privacy.

The Courts clearly still feel bound to express the law in traditional terms "breach of confidence" although steps are being taken towards a fully fledged privacy law, whatever terminology may now be chosen (misuse of private information).

McKennitt confirmed that the application of Article 8 imposes not merely negative but also positive obligations on the state: to respect and therefore to promote the interests of private and family life. It is now accepted law that the Courts must not act "in a way which is incompatible with a Convention right".[25]

As a result, the rules of the English law of breach of confidence also require us to look in the jurisprudence of Articles 8 and 10 which are the very content of the domestic tort that the English courts have to enforce. The correct way to view the contest between the two Articles is:-

The significance of the interference with Article 8 rights which would result from publication against the significance of the interference with Article 10 rights that would result from prevention of publication.

Whilst recent Judgments may not be welcome in the eyes of the media and those who regard freedom of expression to be an ultimate priority, they have to some extent clarified the law and brought it in line with the European position.

Some questions do remain unanswered, not least the precise nature of the privacy right: is it a personal right which cannot be assigned or a property right? In *Douglas*[26], in rejecting OK!'s claim, the Court of

[25] Human Rights Act 1998, Section 6.
[26] Douglas v Hello, C.A., *Ibid*.

Appeal held that confidential or private information which was capable of commercial exploitation but which was only protected by the law of confidence could not be treated as property that could be owned and transferred. The case has been appealed and the House of Lords judgment is currently awaited.

Ms Ash petitioned the House of Lords for permission to appeal the *McKennitt* decision. However permission was refused and therefore the Court of Appeal decision will stand unchallenged as a leading authority.

This has proved to be a rapidly growing area and in months to come it is likely that there will be further decisions which will add to the growing case law. It is apparent now that in the UK that privacy is entitled to the protection of the law in all but name.

Spilling Your Beans: An Analysis of States' Notice of Breach Laws and Recent Court Rulings

By: Benita A. Kahn
William G. Porter II and
John L. Chaney

I. INTRODUCTION

Consider the following nightmare scenario: A laptop belonging to your company or client is lost or stolen. The laptop might contain the names, addresses, social security numbers, credit card numbers, and other personal information of hundreds of thousands of individuals. Must your company or client notify the potentially affected individuals of this security breach? If so, how, and in which states? Will notifying those individuals expose your company or client to liability for other, related legal and contractual violations? What legal exposure does your company or client face if it fails to properly notify the individuals? What can be done to protect against this potential risk? Where do the courts stand?

The advent of the information society has brought with it numerous legal and societal changes. Information once stored in paper files is now routinely stored on computers or by other electronic means. As a result of this profound change in the manner in which society conducts business and other affairs, personal information such as social security numbers and credit card numbers can more easily be accessed, transported, transmitted and used. All of these benefits, however, bring with them an increased risk of unauthorized access and theft. Unauthorized disclosure of such information carries with it the possibility that criminals will engage in fraudulent use of the information, which carries with it the risk of legal exposure to companies.

Benita A. Kahn is a partner with Vorys, Sater, Seymour and Pease LLP in its Columbus, Ohio office, and practices primarily in the areas of privacy, consumer protection, information security, and telecommunications law. Ms. Kahn works with her clients to strategize and discover the best legal and business solutions for many current issues, including: data security compromise responses, including Notice of Breach compliance, incident response programs, and credit card association processes; privacy policy creation, management and administration; compliance with PCI DSS and other data security laws; contracting issues related to privacy and data security; and, federal and state consumer protection laws, including those concerning Do Not Call compliance, the Telemarketing Sales Rule, other telemarketing laws, text messaging, CANSPAM, advertising and information collection.

John L. Chaney is an associate at Vorys, Sater Seymour and Pease LLP in its Columbus, Ohio office. Focusing primarily on commercial litigation, Mr. Chaney also practices in the areas of constitutional, securities and antitrust law. Mr. Chaney holds a B.S. in Finance from The Ohio State University (1997) and a Juris Doctor from The Ohio University Michael E. Moritz College of Law (2000).

William G. Porter II is the head of litigation in Columbus, Ohio office of Vorys, Sater, Seymour and Pease LLP and practices in all areas of litigation, emphasizing in corporate and business disputes, commercial law, including data privacy breaches, construction and design professional liability law, product liability law, and land use law. Mr. Porter has been a member of the IADC since 1994 and is a frequent lecturer on trial advocacy issues for the IADC.

Even casual observers of the news are likely aware that many instances of data compromises have occurred in the last several years. Reports from the Privacy Rights Clearinghouse indicate that 153 million data records have been exposed since it started keeping track of incidents in 2005.[1] Several high profile instances of security breaches have occurred over the last several years, for example:

- In February, 2005, ChoicePoint, a data management company that maintains and sells information on hundreds of millions of Americans, disclosed that it had been deceived by individuals posing as legitimate businesses into disclosing the personal information of approximately 145,000 consumers nationwide, including names, addresses, social security numbers, credit reports, and other information. [2] The Federal Trade Commission announced in 2006 that ChoicePoint will pay $10 million in civil penalties for violation of the Fair Credit Reporting Act and $5 million in consumer redress in a consent decree with the FTC .[3]

- In June, 2005, a class action lawsuit was filed in California state court against credit card payment processor CardSystems Solutions, Mastercard, Visa, and Merrick Bank, a card-issuing bank that used CardSystems to process transactions. The suit alleges the defendants failed to properly notify entities and individuals that were affected by a data breach at CardSystems that compromised approximately 40 million credit card accounts. The case has not yet been resolved, but plaintiffs are seeking damages for injuries incurred as well as payment for credit-monitoring services.[4]

- In early 2006, a laptop belonging to an employee of the Veterans' Administration was stolen from his home. The laptop contained personal data of millions of U.S. veterans, including social security numbers. The Veterans' Administration announced again in February 2007 that unauthorized access had resulted in the exposure of billing information of 1.3 million doctors providing services to veterans.[5]

- In its 2007 SEC filings, TJX described the results of its investigation of a data compromise that occurred at its retail outlets. The unauthorized access to its computer network commenced in July 2005, but was not discovered until December 2006. Information from more than 46 million credit cards (including magnetic stripe information in more than half of these cards) and driver's license numbers, names and addresses of more than 450,000 customers was stolen. This has so far resulted in 19 law suits being filed against TJX and an investigation by the Federal Trade Commission and 30 state Attorneys General. As of the date of the filing of its 10-K, TJX had recorded a pre-tax charge of 1¢ per share.[6]

---

[1] Privacy Rights Clearinghouse, A Chronology of Data Breaches (Apr. 22, 2007), at http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP.

[2] *See* Bob Sullivan, Data Theft Affects 145,000 Nationwide, Feb. 18, 2005, available at http:www.msnbc.msn.com/id/6979897.

[3] *See* Federal Trade Commission, Press Release, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, available at http://www.ftc.gov/opa/2006/01/choicepoint.htm.

[4] *See* Joris Evers, Security Strategy, Mastercard Data Breach: Lawsuit Demands Damages, July 7, 2005, available at http://software.silicon.com/security/0,39024655,39150141,00.htm; Brian Krebs, CardSystems Hit With Class Action Lawsuit, June 28, 2005, available at http://blog.washingtonpost.com/securityfix/2005/06/cardsystems_hit_with_class_act.html.

[5] *See* Privacy Rights Clearinghouse, *supra* note 1.

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

- In March and April 2007, the Texas Attorney General announced the filing of lawsuits against Radio Shack and CVS. In both cases, the complaints alleged that customer information, including social security numbers, credit card numbers, names, addresses and medical information, was found in dumpsters behind store locations. The Attorney General asserted these incidents were violations of Texas laws that require businesses to develop retention and disposal procedures for customer personal information and that require the protection and proper disposal of sensitive personal information.[7]

In response to these and other well-publicized instances of theft or inadvertent disclosure of personal information, states began implementing legislation a few years ago to require businesses or other persons which own more sensitive personal information to notify individuals when a security breach has resulted in disclosure of their sensitive personal information. California was the first state to enact such legislation in 2002, and since 2005 a majority of states have followed suit.[8] As breaches in the security of sensitive personal information increase in frequency and scope, more states and perhaps the federal government are likely to follow suit with their own notice of breach laws. This patchwork of various states' laws and the likelihood that companies are more susceptible to an inadvertent breach creates the possibility of extensive and costly litigation for companies. A proper understanding of legal responsibilities and potential penalties will help prepare and insulate companies when a breach of data security occurs. Just as important is putting in place a good process to assess a company's data security status and an incident response plan in the event of a suspected compromise.

This article provides a primer on the various notice of breach statutes states have enacted by addressing: (1) what information is deemed "personal information; (2) what constitutes a "breach of security" of personal information; (3) what notice, if any, is required in the event of a breach of security; and, (4) what liability may be incurred in the event of a violation. In addition, this article discusses how companies detecting a security breach may find themselves in the unwelcome position of having to admit to a possible violation of other laws resulting from compliance with notice of breach legal requirements. Adding to the complexity, choice of law issues may challenge companies with multistate operations to clearly understand whether and where notification is required and, if it is required, what form it should take. This article provides a brief discussion of a likely choice of law scenario companies may encounter and the corresponding legal framework. Finally, suggestions are provided for implementing a process to address data security and creating an incident response plan.

II. ANALYSIS OF VARIOUS STATE LAWS

Although the various state notice of breach statute contains slight differences, the basic framework of the laws is fairly similar. Generally, notice of security breach laws provide that a data security breach has occurred *if as a result of a breach of a security system there has been unauthorized acquisition of and/or access to unencrypted computerized data that compromises the security, confidentiality or integrity of*

[7] Juan A. Lozano, Texas AG: CVS Dumped Customers' Records, Apr. 17, 2007, available at http://biz.yahoo.com/ap/070417/tx_cvs_identity_theft.html?.v=1.

[8] As of April 2007, 36 states have passed notice of breach laws.

sensitive personal information maintained by the person or business.[9]

A. Personal Information

To limit the applicability of these notice laws to more sensitive personal information, most states provide a baseline definition of "personal information" as an individual's name (first name or first initial, and last name) in combination with at least one of the following: social security number, driver's license number or state identification number, and account number, credit card number, or debit card number.[10] While most states indicate the account number, credit card number or debit number are to be in combination with some security or access code to permit access, it has generally been interpreted by the states that since no such code is "necessary" to access a credit card account, the credit card number alone is sufficient to meet this definition. In most instances, states specifically exempt from the definition information that is publicly available through government records.[11] Some states define "personal information" to include, in addition to a first and last name, a middle and last name.[12] Others define "personal information" as any of the items listed in the general definition above, even if a name is not disclosed, when the information disclosed is sufficient to perform or attempt to perform identity theft. Similarly, at least one state provides that dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.[13] Several states include in the definition date of birth, maiden name, digital signatures, or employer identification numbers.[14]

In likely anticipation of future means of identity theft, certain states have broadened their definition of "personal information" to include physical data. This also reflects that notice statutes have been enacted over a several year period, allowing more types of sensitive data to be considered. For example, a few states include in the definition individually identifiable medical information.[15] Other states include in the definition of personal information unique biometric data, such as fingerprints, voice prints, or retina or iris image, or any other unique physical representation.[16] One state even includes in the definition of "personal information" a person's DNA profile.[17]

The examples provided above are by no means exhaustive. In the event of a potential breach, a careful review of the laws of each state involved in the compromise is necessary to determine whether, under the state's definition, the information disclosed constitutes "personal information." As discussed *infra* at 12, a company may expose itself to liability for other statutory violations when it notifies an individual that the individual's personal information has been disclosed.[18]

---

[9] *See, e.g.,* Cal. Civ. Code § 1798.82(d) (2007); I.C. § 28-51-104(2) (2007); O.R.C. § 1349.19(A)(1)(a) (2007).

[10] *See, e.g.,* Cal. Civ. Code §1798.81.5(d)(1) (2007); I.C. § 28-51-104(5) (2007); O.R.C. §1349.19(A)(7)(a) (2007).

[11] *See, e.g.,* Cal. Civ. Code § 1798.81.5(d)(3) (2007); I.C. § 28-51-104(5) (2007); O.R.C. § 1349.19(A)(7)(b) (2007).

[12] F.S.A. § 817.5681(5) (2007).

[13] N.J.S.A. 56:8-161 (2007).

[14] *See, e.g.,* N.C.G.S.A. §75-61(10) (2007); NDCC, 12.1-23-11(1) (2007).

[15] *See* A.C.A. § 4-110-103(7)(D) (2007); 6 Del.C. § 12B-101(2)(iv) (2007).

[16] Neb. Rev. St. § 28-608(4)(b) (2007); W.S.A. 895.507(1)b)(5) (2007).

[17] W.S.A. 895.507(1)(b)(4) (2007).

[18] This Article generally refers to companies or persons when discussing application of notice of breach laws, but states also vary as to which types of entities are subject to their laws. For example, Georgia's notice of breach law applies only to "information brokers," whereas Oklahoma's notice of breach law regulates only government entities. On the other end of the spectrum, some states apply their laws to any entity that handles, collects, disseminates or otherwise deals with personal information. As a general rule, however, companies

B. Definition of "Security Breach"

Generally, for notice of breach law purposes, states define a security breach as the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the person or business.[19] Most states exempt from the definition of security breach the good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, provided the personal information is not otherwise used or subject to further unauthorized disclosure.[20]

The differences in the various states' laws regarding the definition of a "security breach" are less than those applicable to the definition of "personal information," but some variances do exist. For example, a majority of states provide that a breach occurs only when computerized or electronic data is accessed, while some include in the definition access to or acquisition of personal information contained in non-electronic files, such as paper, audiotapes, photos, or microfiche.[21] For those states limiting the reach of their laws to computerized or electronic data, all currently define a breach as occurring only when the data accessed or acquired was not encrypted.[22] Some states do provide that if the encryption key is also stolen, then a breach has occurred.[23] Likewise, at least one state provides an exception for laptops on which personal information is stored if access to the laptop (or other portable electronic device) is protected by a password that has not been disclosed.[24] In addition, some states provide that a breach has not occurred if the data, whether computerized or otherwise, is redacted in some form.[25]

Frequently, a person or business might be uncertain whether there was an unauthorized access to or acquisition of personal information and, if a breach did occur, whether it is reasonably likely the personal information will be used in a manner to harm the affected individual. For example, there have been numerous thefts of laptops where it was unknown if the theft was for the equipment or the data.[26] It is also possible in some cases that there may be an indication of a "common point of purchase" and vulnerabilities in the security of the system, but no proof that those vulnerabilities were exploited.

Acknowledging this reality, some states incorporate language providing that a breach has occurred when personal information has been accessed or acquired in an unauthorized manner *or* when a person or company has *a reasonable basis* to conclude that personal information has been accessed or acquired in an unauthorized manner.[27] Companies

should expect to be subject to the various states' notice of breach laws.

[19] *Supra*, note 9.

[20] *Id.*

[21] *See* HRS § 487N-1 (2007); IC 24-4.9-2-2(a) (2007).

[22] In April, and as a result of the TJX compromise, a House Legislative Committee in California approved an amendment to the California notice of breach law to delete "unencrypted" from its definition of breach of a security system. *See* Donald G. Aplin, TJX Breach Prompts Committee OK of Bill to Amend California Breach Notice Law, 6 BNA PRIVACY AND SECURITY LAW REPORT 653, 667 (Apr. 23, 2007).

[23] *See* N.H. Rev. Stat. § 359-C:19(II) (2007); McKinney's Gen. Bus. Law § 899-aa(1)(b) (2007).

[24] IC 24-4.9-2-2(b)(2) (2007).

[25] It is unclear whether an incomplete social security or other number combined with a person's name is "redacted" for these purposes. Some, but not all, notice of breach states exempt "redacted" social security numbers from the definition of personal information. In some of these states, "redacted" is not defined. In those states that have defined the term, such as Ohio, a redacted social security number is one in which all but the last four digits of the number have been removed. *See* O.R.C. §1349.19 (A)(9) (2007).

[26] Privacy Rights Clearinghouse, *supra* note 1.

[27] *See, e.g.,* A.R.S. § 44-7501(A) (2007); C.R.S.A. §6-1-716(1)(a) (2007).

operating in states having such "reasonable basis" provisions in their definitions of a breach should likely assume they have a duty to investigate in good faith and in a reasonable manner whether such a "reasonable basis" exists. Similarly, some states deem a breach to occur only when the unauthorized acquisition of or access to computerized data *materially* compromises the security or confidentiality of personal information.[28] In these states, whether a disclosure is "material" would appear to depend on the circumstances. Moreover, statutes requiring companies to make these subjective judgments necessarily suggest that companies make decisions with an awareness that those decisions may subsequently be second-guessed in a lawsuit.

C. Duty to Notify

Most states provide that, if a breach has occurred, notice is required and must be made in the most expedient manner possible and without unreasonable delay.[29] In these states, a duty to notify always arises when there has been an unauthorized disclosure, unauthorized acquisition of or unauthorized access to personal information. However, many states have enacted risk-based statutes that, generally, condition a duty to notify upon an assessment of whether there is a risk that the individual whose personal information was disclosed may be harmed.[30] Some "risk-based" states specify the risk feared is identity theft, or fraud, or both, or, more generally, whether the personal information has been or will be misused.[31] A subset of these "risk-based" states provide that any risk of harm determination must be made in consultation with law enforcement officials.[32]

In addition, for both risk-based and non-risk-based states, statutes often require that an entity conduct an investigation to determine whether a breach has occurred or whether the risk of harm rises to a level where notification must occur.[33] Usually, states provide that the investigation must be conducted in good faith and in a reasonable and prompt manner.[34] If the investigation determines that a breach has occurred or, in some states, is reasonably likely to have occurred, the entity must give notice as soon as possible to the affected resident.[35] Other states provide that notification must occur within a specified number of days following a determination that a breach has occurred; for example, Ohio, Florida and Wisconsin specify notification must occur within 45 days.[36] Furthermore, most states provide that the timely notice requirements of their statute are subject to the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Careful attention must also be paid to the form any notice must take. Some states do not specify what information is required to be provided when notice is given. Other

---

[28] *See, e.g.,* F.S.A. 817.5681(4) (2007); I.C. § 28-51-104(2) (2007).

[29] *See, e.g.* Cal. Civ. Code § 1798.82(a) (2007); I.C. § 28-51-105(1) (2007).

[30] Some states incorporate this risk-based language in their definition of a breach, whereas other states incorporate it into the duty to notify. Generally, as to states in the former category, a breach has not occurred if there is no risk of harm to the individual. As to states in the latter category, although a breach may be deemed to have occurred, a duty to notify arises only when a risk based assessment leads to a determination that the information has been or will be misused. Regardless of whether the risk-based assessment is conducted to determine if a breach has occurred or whether, despite a breach occurring, there is a duty to notify, the practical effect is the same.

[31] *See* I.C. § 28-51-105(1) (2007); K.S.A. § 50-7a02(a) (2007).

[32] N.J.S.A. 56:8-163(c)(1) (2007); Gen. Laws 1956, § 11-49.2-4 (West 2007).

[33] *Supra*, notes 30, 32.

[34] Some states explicitly require that the entity document the assessment made and maintain such documentation for a number of years.

[35] *See, e.g.,* O.R.C. § 1349.19(B)(2) (2007); Gen. Laws 1956, § 11-49.2-3(d) (2007).

[36] O.R.C. § 1349.19(B)(2) (2007); F.S.A. 817.5681(1)(a) (2007); W.S.A 895.507(3) (2007).

states provide in painstaking detail the information required to be in the notice. For example, Hawaii requires the notice to be clear and conspicuous, and to include: the incident in general terms; the type of personal information subject to unauthorized access or acquisition; the general acts of the business to protect the information from further unauthorized access; a phone number for further information and assistance, if one exists; and, advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.[37] From a practical perspective, if credit card information is involved, it is useful to the consumer to include the last four digits of the compromised card in the notice letter. Since many consumers have multiple cards, this will reduce calls to the affected company.

Adding a further wrinkle, some states require that notification must be made to specified government agencies and, in some instances, that such notification must occur before the affected individual is notified.[38] In addition, upon occurrence of a breach affecting a specified number of people (generally over 1,000), some states require that consumer reporting agencies promptly be notified of the timing, distribution, and content of the notice.[39]

The permissible means of notice vary widely across states having notice of breach laws. All states with notice of breach laws permit written notice. Many states also permit notice by electronic means and telephone. Most states also provide for a form of substitute notice in certain circumstances. For example, Utah permits, without exception, notice by publication in a newspaper of general circulation.[40] Other states provide that substitute notice may be given only when the company demonstrates the cost of providing notice would exceed a certain amount, the affected class of persons to be notified exceeds a certain amount, and/or there is insufficient contact information to notify affected individuals.[41] Some of these states permit substitute notice to be provided through local or statewide media, through email, a conspicuous posting of the notice on the company's website, or some combination thereof.[42]

This ability to comply with substitute notice can be very significant when credit card numbers are involved. For example, often when merchants accepting credit card transactions at their stores are facing a compromise, it is unlikely they will have the address of the affected individual. Rather, it is the bank that issued the credit card to the consumer that has the address information, and the merchant does not have a relationship with the issuing bank. In this case, substitute notice may be the only option.

Finally, numerous states provide, generally, that a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of the statute if the person or business notifies affected individuals in accordance with the policy.[43] Due to this notification exception and many other reasons, it is important to have an incident response plan in place.

The response plan notification provisions should be easily understood, practical and appear reasonable to an objective observer. A good incident response plan should also include the following considerations: a quick and efficient means to communicate a possible compromise to the appropriate person(s)

---

[37] *See* HRS § 487N-2 (2007).
[38] N.J.S.A. 56:8-163(c)(1) (2007).
[39] *See* C.R.S.A. 6-1-716(2)(d) (2007); F.S.A. 817.5681(12) (2007).
[40] *See* Utah Code Ann. § 13-44-202 (2006).
[41] *See* Cal. Civ. Code § 1798.82(g)(3) (2007); I.C. § 28-51-104(4)(d) (2007); O.R.C. § 1349.19(E)(3) (2007).
[42] *Id.*
[43] *See, e.g.*, Cal. Civ. Code § 1798.82(h) (2007); C.R.S.A. 6-1-716(3)(a) (2007); F.S.A. 817.5681(9) (2007).

within your company; a committee of those necessary to make the numerous decisions that will be required (e.g., legal, HR, owners of the information, information technology, loss prevention, communications); a means to contain and limit the exposure (e.g., do not alter or turn off the compromised systems, rather isolate them); preservation of logs; keeping a log of actions taken; deployment of mitigation to once again secure the system; evaluation of the need for a forensic investigation; control of intra-company communications; identification of notification obligations (including contractual obligations and, if applicable, SEC filings); preparation for deployment of notices, including preparation of FAQ's for your call center. Upon creation of such policies and procedures, persons or companies must adhere to them and provide any required notice in a timely manner.

Of course, the duty to notify must also take into consideration the practical reality of the company's relationship with its customers and/or employees. Compliance with statutes might only require notice to a portion of the individuals affected by the compromise. As Choicepoint learned, to maintain the important customer and employee relationship and the company's credibility, once it is determined notice must be given to some of the affected individuals, it must be given to all the affected individuals.

D. ENFORCEMENT

As with all aspects of the states' notice of breach laws, civil enforcement provisions vary widely. Nearly every state provides that the state's Attorney General may institute an action. Some states permit other government officials to bring actions as well, including county and district attorneys, and attorneys from states' Consumer Protection divisions.[44] A sizeable minority of states expressly provide for a statutory private right of action by affected individuals,[45] and it is possible that in those states failing to provide for a private right of action individuals might sue under other legal theories.

The prescribed civil penalties in some states are potentially massive in cases of widespread breaches. For example, Texas provides that a person or business who violates the notice of breach statute is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation.[46] Although somewhat unclear, and not yet interpreted by Texas courts, Texas appears to deem a violation as a failure to notify an affected individual. As noted previously, the Texas Attorney General has recently filed lawsuits against Radio Shack and CVS for inappropriately dumping personal information, so this may soon be considered by a court. Other states appear to impose a penalty based on the number of security breaches that occur rather than on the number of individuals who were not notified. Many states permit the Attorney General or other litigant to seek an injunction.

In states permitting a private right of action, injured residents may recover, depending on the state, damages for injuries incurred, treble damages, punitive damages, and attorneys' fees.[47] Some states even deem a violation of the duty to notify affected individuals as a deceptive act, actionable under the state's Unfair or Deceptive Trade Practices laws.[48]

In states that have not enacted a notice of breach law and, perhaps, in states with notice of breach laws that permit a private right of action, individuals might sue under

[44] *See, e.g.,* 6 Del.C §12B-106 (2007); HRS § 487N-3(a) (2007).

[45] *See, e.g.,* Cal. Civ. Code § 1798.84(c) (2007); 6 Del.C § 12B-104(a) (2007); HRS § 487N-3(b) (2007).

[46] *See* Tex. Bus. & Com. Code Ann. § 48.201 (Vernon 2005). Some states place a cap on this liability, but even these caps can be $1 million.

[47] *See, e.g.,* 6 Del. C. § 12B-104(a) (2007); HRS § 487N-3(b) (2007).

[48] *See, e.g.,* NDCC, 51-30-07 (2007); 73 P.S. § 2308 (2007).

common law theories of tort to recover for damages stemming from a failure to notify those individuals that their personal information has been compromised. Recently, Courts have addressed cases involving data compromises of various types.[49] The types of compromise include a home burglary of an employee's laptop that held student loan information, several cases involving retail data compromises, theft of a server from a corporate office, employee theft, and thefts occurring at a service provider's location. In several of the cases, the plaintiffs requested class certification. Plaintiffs in these cases have asserted breach of contract (both implied and as a third party beneficiary), breach of fiduciary duty, negligence (based on an asserted duty of care under Gramm-Leach-Bliley and Visa Operating Regulations), equitable subrogation, promissory estoppel, unjust enrichment, bailment, conversion and claims based on various state and federal credit and consumer protection laws.

To date, the courts have ruled in favor of the defendants in the majority of the decisions. The most consistent basis for dismissal or granting of summary judgment has been the failure to establish Article III standing.[50] This determination has been after consideration of the three elements for standing: suffering an injury-in-fact; a causal connection between the conduct and the injury; and the injury will be redressed by a favorable decision. In each case where the court ruled there was a lack of standing, the court determined that there was no concrete or actual injury, with one court specifically stating that an increased risk of identity theft in the future does not satisfy the element of injury-in-fact.[51] Other rulings for defendants have been based on a lack of cognizable damages, the contracts specifically exclude third party beneficiary rights or the plaintiff was deemed only an incidental beneficiary, the economic loss doctrine, the replacement of credit cards by the issuing bank being deemed a contractual obligation of the bank resulting in no equitable indemnification or unjust enrichment, and a determination that a business transaction does not establish a fiduciary duty.

Two cases in which courts ruled for the plaintiffs involved unusual factual issues. In one case, a relative of a union treasurer stole personal information of the union members and used it for identity theft.[52] The court determined that there was a duty of care and a breach of this duty, but noted that each case will be unique with respect to the duty of care. In *Metropolitan Life Insurance*, the court noted that the privacy policy given to the plaintiff prior to her providing personal information specified

[49] *See, e.g.*, Randolph v. ING Life Ins. and Annuity Co., No. 06-1228 (CKK), 2007 WL 565872 (D. D.C. Feb. 20, 2007); Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); Key v. DSW Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006); Giordano v. Wachovia Securities, LLC, No. 06-476 (JBS), 2006 WL 2177036 (D. N.J. July 31, 2006); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775 (W.D. Mich. 2006); Pennsylvania State Employees Credit Union v. Fifth Third Bank, No. 1:CV-04-1554, 2006 WL 1724574 (M.D. Pa. June 16, 2006); Banknorth v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206 (M.D. Pa. 2006); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006); Guin v. Brazos Higher Ed. Service Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006); Richardson v. DSW, Inc., No. 05 C 4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005); Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005).

[50] *See* Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); Key v. DSW Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006); Giordano v. Wachovia Securities, LLC, No. 06-476 (JBS), 2006 WL 2177036 (D. N.J. July 31, 2006); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006); Stollenwerk v. Tri-West Healthcare Alliance, No. Civ. 03-0185PHXSRB, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005).

[51] Key, 454 F. Supp. 2d at 688-89.

[52] Bell v. Michigan Council 25 of American Federation of State, County, Municipal Employees, AFL-CIO, Local 1023, No. 246684, 2005 WL 356306 (Mich. App. Feb. 15, 2005).

that the company "took great care in safeguarding [its] customers' personal information".[53] The court then imposed a duty of care, but determined it was a question of fact for the jury to decide the amount of damages and the relevance of the intervening acts of the third party thieves.[54]

E. RELATED STATUTORY PROVISIONS

Many states include in their statutory scheme related provisions covering security procedures to protect against breaches in the first instance and requirements that records containing personal information be destroyed in a certain manner. For example, Arkansas and some other states provide that businesses that own personal information "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[55] California, for example, requires a written information security program if one collects personal information, as defined by the California notice of breach law, from California residents. Likewise, Arkansas and fifteen other states require that businesses take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.[56] Each of these requirements impose a duty upon companies or persons owning or possessing personal information, the violation of which may be actionable for damages.

Similarly, many states have restricted the use of social security numbers, and violations of these statutes may result in injunctive relief and civil penalties. Most states prohibit the public display or posting of an individual's social security number, printing the number on any card or document required to gain access to products or services, requiring the transmission of the social security number over the Internet unless the connection is secure, requiring an individual to use his or her social security number to access an Internet website unless a password or personal identification number is also used, or printing an individual's social security number on materials mailed to the individual. Remedies for violations of these statutes include injunctions, civil penalties of up to $5,000 per violation, and the creation of a private right of action. In Michigan, the unlawful use of a social security number is a crime, punishable by up to ninety-three days imprisonment or a fine of not more than $1,000, or both.[57] Michigan also provides that an individual may bring a civil action against a person for a violation of the social security number disclosure provisions, recover actual damages and, for knowing violations, minimum damages in the amount of at least $1,000 and reasonable attorney fees.[58]

Companies and persons subject to these and other related laws may find themselves in the unwelcome position of notifying individuals that there has been an unauthorized access to or acquisition of their personal information. However, in doing so, companies may be handing potential plaintiffs a valuable admission to use against them during litigation. Companies thus may find themselves in the proverbial catch-22 situation, obligated to notify affected individuals of a disclosure of

[53] Daly v. Metropolitan Life Ins. Co., 782 N.Y.S. 2d 530, 536 (2004).
[54] *Id.* at 536-37.
[55] A.C.A. § 4-110-104 (2007).
[56] *Id.*
[57] *See* Mich. Comp. Laws §§ 445.83, 445.86 (2005).
[58] *Id*.

their personal information but, as a result of such notification, exposed to potential liability for other, related violations.

Two hypothetical but painfully realistic scenarios illustrate the bind in which companies may find themselves. One obvious situation that a company might encounter arises when that company becomes aware of an unauthorized access to or acquisition of personal information held by the company and the company must determine whether, in a risk-based state, the potential for harm resulting from the breach requires the company to issue notifications. However, that same state may also require companies to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Though certainly not *prima facie* evidence that the statute requiring implementation and maintenance of reasonable security procedures has been violated, such notification will certainly alert enterprising counsel that a colorable claim may exist. Of course, the security breach may become public in any event and thus subject a company to claims that both provisions have been violated. In fact, one of the lawsuits filed against TJX Companies included allegations that TJX failed to properly secure information and then failed to notify affected consumers upon discovery of the security breach.

In another situation, a state may prescribe penalties for improper disclosure or use of a social security number. If the personal information that has been accessed or acquired in an unauthorized manner is a social security number, the company may find itself admitting to a violation of the social security number law when it notifies individuals of the security breach.

In both situations, the company lacks attractive options. If the company, after a thorough and reasonable investigation, determines there is no risk of harm to affected individuals due to the breach, it may avoid this Hobson's Choice. However, if the situation remains unclear after a proper investigation, the company will have to make the difficult decision of whether to notify affected individuals and thus risk a lawsuit. Yet, failure to notify affected individuals in situations where the risk of harm is unclear may subject the company to a suit for violating both the notice of breach law and related laws.

III. JURISDICTIONAL ISSUES

Several jurisdictional and related issues will arise as plaintiffs and the bar become aware of the causes of action that may be asserted pursuant to the recently enacted notice of breach laws. In particular, choice of law issues are certain to play a significant role in the resolution and litigation of such disputes because of the ever expanding multistate character of modern corporations.

The following scenario illustrates some choice of law issues that may arise. Careless Corporation, a consumer data broker headquartered in State X, learns that a company laptop containing the names and social security numbers of tens of thousands of consumers nationwide may have been lost or stolen. To some degree, Careless conducts business in all fifty states and possesses data about consumers residing in all fifty states. Upon learning of the missing laptop, Careless' management orders an intensive investigation to determine its whereabouts and how it went missing. Even after a thorough investigation, Careless remains uncertain whether the laptop is simply missing or whether it was stolen. Careless must now determine its legal obligations and, in particular, whether each consumer whose data was on the laptop must be notified of a security breach.

As an initial matter, Careless should determine whether its home state has enacted a notice of breach statute. If so, Careless should next determine whether its home state notice of breach statute requires Careless to notify residents of other states.

If Careless' home state does not require notice to residents of other states, which is the general rule, Careless must analyze and determine whether, under potentially applicable choice of law principles, it is required to comply with notice of breach laws enacted by those other states. The situation may be further complicated if Careless' home state enacted a risk-based statute. Careless must then "reasonably determine" whether the loss or theft of the laptop poses a risk of harm to the affected individuals. In that situation, Careless will have to decide whether, pursuant to its home state law, it has a legal obligation to notify affected consumers, and whether other states' laws require Careless to provide notice in all instances where there has been an unauthorized access to or acquisition of personal information of that state's residents. Adding to the complexity, Careless' home state may have enacted a statute providing for civil liability for each instance of an unlawful use or disclosure of social security numbers. Careless is thus torn —it may reasonably decide it has no duty to notify consumers pursuant to its home state law, is potentially liable for each instance of improper disclosure of social security numbers if it does notify consumers, and may be compelled by certain states to notify those states' residents. In short, unless Careless is willing to notify affected individuals nationwide, Careless must undertake a careful and thorough choice of law analysis.

Unfortunately for Careless, states also differ in how they approach choice of law analyses. Thus, depending on the state where any action is filed, Careless may receive different court decisions on which state's law is to apply. Yet, Careless is not without sources of guidance. Many states follow the Restatement, Conflict of Laws, § 6, which provides that courts should inquire into the following factors in determining which state's law should apply:

> (1) A court, subject to constitutional restrictions, will follow a statutory directive of its own state on choice of law.
>
> (2) When there is no such directive, the factors relevant to the choice of the applicable rule of law include:
>
> (a) the needs of the interstate and international systems,
>
> (b) the relevant policies of the forum,
>
> (c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue,
>
> (d) the protection of justified expectations,
>
> (e) the basic policies underlying the particular field of law,
>
> (f) certainty, predictability and uniformity of result, and
>
> (g) ease in the determination and application of the law to be applied.

In applying the above factors, as with any choice of law issue, Careless should research how the Restatement factors have been applied in analogous situations. Aside from such precedent, however, plaintiffs' counsel in a suit challenging Careless' failure to notify can be expected to make strong arguments for applying the laws of the foreign state if those laws are favorable to plaintiffs' position.

As an initial matter, Careless can be expected to argue that its home state forum has expressed, through legislation, a strong policy preference that its laws apply to any breach that has occurred. Furthermore, Careless can be expected to argue that it faces an impossible task of properly applying fifty states' laws to breaches affecting residents of those states. Subtle variations between the states' laws and applicable case law could create a trap for Careless, perhaps causing its determination that there is no risk of harm to affected individuals to be unreasonable in another risk-based state. Such uncertainty, Careless

would argue, would not serve the needs or interests of the interstate system, the goals of certainty, predictability and uniformity of result, and the goal of ease in the determination and application of the law to be applied.

Conversely, plaintiffs attempting to have their home state's law applied would likely argue that their jurisdictions have also, through legislation, expressed a strong policy preference that their residents be protected from and notified of disclosures of those residents' personal information. Plaintiffs could argue that, if Careless and similar entities are subject only to their home states' notification laws, foreign state residents are protected only in the rare and entirely arbitrary situation where the disclosing entity is a corporation domiciled in their state, a situation certainly not in accord with the intent of the respective state legislatures in enacting the notice of breach laws. Plaintiffs can also be expected to point out that, to some degree, Careless does business in plaintiffs' home state, receives benefits from doing so, and should thus be subject to plaintiffs' state's notice of breach law. Moreover, plaintiffs can be expected to highlight the perverse incentive a contrary ruling would entail, *i.e.*, that companies possessing or owning personal information would have an incentive to incorporate in a state lacking a notice of breach law. These and other arguments would likely be made by both sides to the dispute, and it is unclear how courts would rule on the issue.

A case in point is the Supreme Court of California's recent decision in *Kearney v. Salomon Smith Barney, Inc*.[59] There, the Supreme Court of California decided whether Georgia or California's law would apply to a suit alleging that employees at the Atlanta, Georgia, branch of Salomon Smith Barney had illegally recorded telephone conversations with plaintiffs, who were California residents, without plaintiffs' consent. Noting that Georgia's statute does not prohibit the recording of a telephone conversation when the recording is made with the consent of *one* party to the conversation, but that California's statute requires the consent of *all* parties to the conversation, the court found a classic conflict of laws. In analyzing the issue, the court first stated that it applies a "governmental interest analysis," wherein the court inquires as to which jurisdiction's interests would be more severely impaired if that jurisdiction's law were not applied in the particular context presented by the case.[60] In finding that California's privacy law should apply, the court noted several factors articulated in the Restatement. Perhaps foremost in the court's collective mind was California's strong and clearly expressed interest in protecting its citizens' privacy.[61] In addition, the court reasoned:

> individual states may adopt distinct policies to protect their own residents and generally may apply those policies to businesses that choose to conduct business within that state. It follows . . . that, at least as a general matter, a company that conducts business in numerous states ordinarily is required to make itself aware of and comply with the law of a state in which it chooses to do business.[62]

Further, addressing the argument that application of California law to activities of a company in Georgia would constitute a disfavored extraterritorial application of the California statute, the court reasoned, "[a] person who secretly and intentionally records such a conversation from outside the state effectively acts within California in the same way a person effectively acts within the state by, for example, intentionally shooting a person in California

[59] 39 Cal.4th 95 (2006)

[60] *Id.* at 100.
[61] *Id*. at 124.
[62] *Id*. at 105; *see also id.* at 126 (citing Watson v. Employers Liability Assurance Corp., 348 U.S. 66, 72 (1954)).

from across the California-Nevada border."[63]

The *Kearney* court also offered a glimpse of how it might address a choice of law issue concerning application of California's notice of breach law. The court stated that if the law at issue, "and, by analogy, other similar consumer-oriented privacy statutes that have been enacted in California – could not be applied effectively to out-of-state companies but only to California companies, the unequal application of the law very well might place local companies at a competitive disadvantage with their out-of-state counterparts."[64] Another important factor in the court's decision was that California law is more protective of privacy interests than Georgia law and, thus, application of California's law would not violate any privacy interest protected by Georgia law.[65]

Some of the other factors considered by the court in arriving at its holding are inapposite to a consideration of which states' laws would apply in the notice of breach context, but *Kearney* does provide a thoughtful opinion that can, by analogy, serve to highlight several of the factors courts might consider in determining which states' notice of breach law should apply in a given situation. Reflecting the uncertainty inherent in any choice of law determination, however, the *Kearney* court noted that courts from four other jurisdictions had reached differing conclusions as to which state's eavesdropping laws should apply.[66]

IV. CONCLUSION

Notice of breach laws are a recent legislative phenomenon and promise to prove fertile ground for litigation for enterprising counsel and aggrieved or litigious plaintiffs. With identity theft becoming one of the fastest growing offenses in the country, businesses must protect personal information in their possession and, if disclosure of that information occurs, carefully assess their legal responsibilities to notify the affected individuals. An error in judgment or failure to understand the states' widely varying statutes can subject companies to extensive litigation and the possibility of significant monetary awards.

A better plan is to implement a process to assess risk, implement a security plan and continue to assess and address risk on an ongoing basis. In this respect, the following important considerations will help reduce the possibility of exposure to a compromise:

- Collect and retain the minimum amount of personal information for business needs;
- Inventory where personal information is located in the company systems, including higher risk laptops and other portable devices (consider all stages – collection, use, disclosure, retention, disposition);
- Classify personal information based on its sensitivity and implement appropriate physical, technical and administrative safeguards based on the classification of the personal information;
- Limit access to sensitive personal information to only those employees with a need to know;
- Create employee training and communications about security awareness;
- Impose obligations on service providers and vendors with access to personal information, based on the classification of the personal information;
- If encryption is used, focus on the key management as well; and
- Properly dispose of personal information and the equipment containing personal information.

Finally, it is important to remember that the task of data security is never done.

---

[63] *Id*. at 119.
[64] *Id*. at 126.
[65] *Id*. at 126-27.
[66] *Id*. at 129 & n.16.

The Privacy Project III

Police Confidential: Access to Law Enforcement Files in New York Federal Court Actions

By: Paul E. Svensson and John J. Walsh

Introduction

The purpose of this article is to provide an overview of the issues that confront law enforcement personnel relative to the demand for information and records, and to prepare their attorneys to defend against unwarranted disclosure and insure proper *in camera* inspection by the courts.

While certain commentators express views that open access is the only effective check on the abuse of police power,[1] unfettered public access to records and information complied in investigation of suspected crime; police personnel, training and medical reports; and internal investigations could violate personal privacy rights and prejudice effective enforcement of law and order.

Discovery Demands

The Freedom of Information Act (F.O.I.A.), Federal Rules of Civil Procedure and judicial interpretation govern access to records and information complied for law enforcement purposes.

In federal actions, discovery is expected to be broad, and all relevant materials, which are reasonably calculated to lead to the discovery of admissible evidence, are generally discoverable.[2]

Paul E. Svensson is a Partner in Hodges Walsh & Slater, LLP, 75 South Broadway, White Plains, New York. A graduate of Pace University School of Law, he practices in land use and civil rights defense, and all aspects of appellate work.

John J. Walsh is a Partner in Hodges Walsh & Slater, LLP, 75 South Broadway, White Plains, New York. A graduate of Fordham University School of Law, he is a seasoned trial attorney who practices in municipal defense and constitutional law. He is a member of the IADC.

Under Rule 26(b)(1), "[p]arties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party." Moreover, "[r]elevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."[3]

Discovery demands are likely to include requests to produce police academy and other training files; employment applications, records of interviews, pre-employment investigation, and other documents contained in personnel files, including psychological test results and medical reports; internal investigation records and documentation of any disciplinary actions; performance monitoring and fitness for duty evaluations; use of force records; civilian complaint files; and documents concerning prior law suits concerning abuse of lawful authority, false swearing, excessive force, assault, battery, false arrest, malicious prosecution, malicious abuse of process or violation of any constitutional rights.

---

[1] Prime, Jamison S., A Double-Barreled Assault: How Technology and Judicial Interpretations Threaten Public Access to Law Enforcement Records, 48 Fed. Comm. L.J. 341 (1996).

[2] Fed. R. Civ. P. 26; S*ee* National Congress for Puerto Rican Rights v. City Of New York, 194 F.R.D. 88, 91 (S.D.N.Y. 2000);

[3] Fed. R. Civ. P. 26(b)(1).

As will be discussed further below, the courts have broad discretion in deciding what is, or is not, discoverable.[4]

Responding to Demands for Privileged Information

Pursuant to Fed. R. Civ. P. 33, and subject to local rules, responses are due within 30 days and a detailed privilege log must accompany all objections. *Pro forma* invocation of privilege is "discouraged," and interpreted as impermissible.[5] In the case of the Southern and Eastern District Courts for the State of New York, a similar procedure is often used to evaluate a claim of privilege.[6]

In *King v. Conde*, the Honorable Jack B. Weinstein set forth a procedure and test "designed to govern all discovery disputes over police records in federal civil rights actions in [the Eastern District of New York], regardless of the label used to refer to the privilege."[7]

Judge Weinstein based the procedure upon the premise that in order to assert a claim of privilege against disclosure of police materials in a federal civil rights claim against a police defendant, the officers or the police department must do more than alert the court to the relevant privilege or the generalized policies which support it. The procedure requires that the police specify which documents or class of documents are privileged, and for what reasons, in the form of a declaration or affidavit.[8] The police must make a "substantial threshold showing that there are specific harms likely to accrue from disclosure of specific materials."[9]

While the procedure described in *King* requires that the affidavit be submitted "from a responsible official within the agency who has personal knowledge of the principal matters to be attested to in the affidavit or declaration," under the circumstances of the majority of actions, subject to local rules, an affidavit or declaration from defendant's counsel will suffice, provided that it is based on personal review of the documents by an official in the police agency and must explain how the materials at issue have been generated or collected; how they have been kept confidential; what specific interests of the police officers, of law enforcement, or of public concern would be injured by disclosure to the plaintiff, to plaintiff's attorney, and the public; and the projected severity of each such injury.[10]

Upon the production of the affidavit or declaration, together with the records demanded, the court will conduct an *in camera* review for their relevance to the instant action.[11]

Evaluating the Relevancy of Discovery Demands Balancing Plaintiff Interests with The Official Information Privilege and Personal Privacy

The broad scope of discovery delimited by the Federal Rules of Civil Procedure is designed to achieve disclosure of all the evidence relevant to the merits of a controversy.[12]

---

[4] Wills v. Amerada Hess Corp., 379 F.3d 32 (2d Cir. 2004); In re Fitch, Inc., 330 F.3d 104 (2d Cir. 2003); Cruden v. Bank of New York, 957 F.2d 961 (2d Cir. 1992).

[5] Unger v. Cohen, 125 F.R.D. 67, 70 (S.D.N.Y. 1989).

[6] It is important to note that a state law enforcement privilege, for example New York State Civil Rights Law 50 (a), do not govern discovery in federal cases. Melandez v. Greiner, 2003 WL 22434101, at *4-7 (S.D.N.Y. Oct. 23, 2003).

[7] King v. Conde, 121 F.R.D. 67, 70 (E.D.N.Y. 1988)

[8] *Id.* at 189-190.

[9] *Id.* at 189; *See* also Kelly v. City of San Jose, 114 F.R.D. 653, 669 (N.D.Cal. 1987).

[10] Fountain v. City of New York, 2004 WL 941242 (S.D.N.Y. 2004).

[11] *Id.* at 2.

[12] Thomas E. Hoar, Inc. v. Sara Lee Corp., 882 F.2d 682, 687 (2d Cir. 1989) (citing Fed.R. Civ. P. 26(b)(1) and advisory committee notes).

First, the Official Information Privilege must temper relevancy.[13] In applying the privilege, the Court will balance the plaintiff's interests in disclosure against the state's legitimate concern of protecting the confidentiality of investigative[14], civilian complaint, and an officer's personnel files from unnecessary intrusion.[15] The factors to be considered are substantially the same as those listed in *King*.[16]

In considering these factors, it should also be kept in mind that "although the privacy rights of the officers are not inconsequential, they should be limited in view of the role played by the police officer as a public servant who must be accountable to public review."[17] Further, "these privacy interests must be balanced against the great weight afforded to federal law in civil rights cases against police departments."[18]

The use of a protective order or stipulation of confidentiality may serve to address many privacy concerns since it is unlikely that plaintiffs will be able to obtain information of comparable quality from any other source."[19]

Courts take different approaches to the discovery of documents implicating prior similar acts (*i.e.*, civilian complaint records).[20] Citing grounds such as relevance, improper similar act evidence, and prejudice, some courts have denied requests to obtain Civilian Complaint Review Board (CCRB), complaints and other similar documents, especially when the complaints are unsubstantiated and unrelated to plaintiff's instant claims.[21]

In *Thompson v. the City of New York*, the court found that incidents involving off-duty motor vehicle accidents, the expiration of a driver's license, attempts to bribe and whether proper custodial records were maintained were irrelevant to the subject matter of the complaint.[22] After *in camera* review, the Honorable Paul A. Crotty held that none of the complaints were substantiated, that the charges in the reviewed materials were not reasonably related to the claims in the instant case, and that the production of these materials would not lead to the discovery of admissible evidence.[23]

The New York District Courts have also consistently held that there are cases where the production of unsubstantiated allegations filed by civilians, similar to those raised in plaintiff's instant complaint,

---

[13] Mercado v. Division of New York State Police, 989 F.Supp. 521, 522 (S.D.N.Y. 1998).

[14] The similarity of the Official Information Privilege and the Federal Freedom of Information Act will be discussed below.

[15] *Id*.

[16] Fountain, *supra* Note 9 at *5.

[17] National Congress, *supra* Note 2 194 F.R.D. 96(quoting King, *supra* 121 F.R.D. at 191).

[18] *Id*. (quoting Soto v. City of Concord, 162 F.R.D. 603, 611 (N.D.Cal. 1995).

[19] *Id.*

[20] Compare Bradley v. City of New York, 04 Civ. 8411, 2005 U.S. Dist. LEXIS 22419, at *3 (Oct. 3, 2005) ("There is no question that civilian complaints, whether or not deemed substantiated, may be significant in an assessment of an officer's qualifications and performance, particularly if the complaints reflect a pattern."), with Mingues v. Bezio, 96 Civ. 5396, 1999 U.S. Dist. LEXIS 12976, at * *3-4 (S.D.N.Y. Aug. 19, 1999) ("[P]rior uses of excessive force by the defendants, if any, have no bearing on the issue of whether they used excessive force against plaintiffs.").

[21] *See, e.g.*, Sealy v. Fishkin, 96 Civ. 6303, 1998 U.S. Dist. LEXIS 20142, at * *9-10 (E.D.N.Y. Dec. 2, 1998) (finding that unsubstantiated civilian complains do not suffice to prove Monell claim); Haya v. City of New York, 93 Civ. 7754, 1995 U.S. Dist. LEXIS 7020, at * *1-2 (S.D.N.Y. May 24, 1995) (finding that the requested documents concerning CCRB complaints were not discoverable because they occurred in the distant past, because none was substantiated, and because none involved conduct similar to that alleged by the plaintiff); Marcel v. City of New York, 88 Civ. 7017, 1990 U.S. Dist. LEXIS 4094, at *23 (S.D.N.Y. Apr. 10, 1990) ("Unsubstantiated CCRB reports do not demonstrate a breach of a municipality's duty to train or supervise its police.").

[22] Thompson v. The City of New York, 2006 WL 298702 at *3 (S.D.N.Y. Feb. 7, 2006)(recognizing that the wholesale production of unsubstantiated complaints tends to create a danger of prejudice).

[23] *Id*. at *4.

are relevant or may lead to admissible evidence.[24]

In *Barrett v. The City of New York*, Magistrate Judge Kiyo A. Matsumoto of the Eastern District of New York, held that complaints, concerning defendant police officers submitted to a civilian review board more than 10 years before the incidents that gave rise to the present civil rights suit, containing similar charges as those alleged in the civilian complaints, were not barred from discovery by content, or age, and may still be relevant to establish a pattern of behavior or knowledge by the city of defendants' propensity for such behavior relative to plaintiff's *Monell*[25] claim.[26]

Judge Matsmoto also found that complaints which contained unsubstantiated claims on matters other than those included within plaintiff's complaint were irrelevant and not subject to disclosure.[27]

Similarly, in *Pacheo v. the City of New York*, plaintiff, who brought a suit against city police officers for false arrest and excessive force, and a *Monell* claim against the city, sought full disclosure of all complaint files. Magistrate Judge Viktor V. Pohorelsky held that the production of records of the city's civilian complaint review board and police internal investigations bureau regarding unsubstantiated allegations of other types of misconduct than those alleged in the complaint were protected. The court reasoned that unsubstantiated allegations regarding false arrest and excessive force may lead to admissible evidence, however, other unsubstantiated complaints – unrelated to plaintiffs' claims – were not discoverable.[28]

Furthermore, as to plaintiff's *Monell* claim, which was based upon the theory that the city ignored evidence that the individual defendants had a propensity to make false arrests and use excessive force, the court held that unsubstantiated instances of misconduct unrelated to false arrest and excessive force were irrelevant. Judge Pohorelsky opined "it is doubtful whether unsubstantiated instances of any kind of misconduct can ever be used to prove a *Monell* claim.[29]

On the contrary, in *Harper v. Port Authority of New York & New Jersey*, Magistrate Judge Ronald L. Ellis, held that even unrelated and unsubstantiated complaint records were not protected from disclosure because plaintiff alleged a *Monell* claim against the municipality and the Port Authority's knowledge of, and response to, defendants' behavior and complaint history was relevant.[30]

The Port Authority contended that unsubstantiated complaints and charges, unrelated to the charges set forth in plaintiff's complaint, should not be disclosed, relying on *Thompson* and *Pacheo.* As noted above, in both those cases, the courts ruled that records relating to unsubstantiated complaints were not discoverable.

Judge Ellis, however, granted plaintiff's unfettered access to all unsubstantiated complaints, whether or not reasonably related to plaintiff's complaint, leaving this issue ripe for eventual resolution by the Second Circuit Court of Appeals.

---

[24] Fountain, *supra* Note 9 at *4-5, clarified by Fountain v. City of New York, 2004 U.S. Dist. LEXIS 12278 (June 30, 2004); *See* also Barrett v. The City of New York, 237 F.R.D. 39 (E.D.N.Y. 2006).

[25] Monell v. Department of Social Services, 436 U.S. 658, 98 S.Ct. 2018, 56 L.Ed.2d 611 (1978)(involving a claim against the municipality based upon an alleged custom or practice of supporting, or ignoring, unconstitutional actions of its employees).

[26] Barrett, *supra* Note 21 at 40.

[27] *Id.* at 40-1.

[28] Pacheo v. The City of New York, 234 F.R.D. 53, 55 (S.D.N.Y. 2006).

[29] *Id.*

[30] Harper v. Port Authority of New York & New Jersey, 2006 WL 1910604 at * 2 (S.D.N.Y. July 10, 2006)(citing cases supporting the broad discretion of the court in directing discovery); cf. Sealy, *supra* Note 16 (finding that unsubstantiated civilian complains do not suffice to prove Monell claim);

In the Eastern and Southern Districts of New York, demands for police academy and other training records,[31] employment, monitoring, performance, evaluation and disciplinary records[32] are considered to be relevant and subject to disclosure. Further, police officers cannot assert a privacy interest in internal investigation materials that relate exclusively to their official conduct.[33]

As a result, defendants must make an express objection to the relevancy of unsubstantiated and unrelated claims when production is first demanded, and request that the court review the record for the purposes of redacting information which is subject to special considerations of privacy, such as family members, home address, personal references, disability or other medical evaluations submitted to the department, and retained in personnel files.

Objections should be made to demands for all complaints, use of force records, on the job injury records, and prior law suits. Plaintiff should be required to produce an explanation to the court as to what they expect the court to find in its review of the records as well as the relevancy to the claims set forth to the instant action. The court must be encouraged to review the records critically and deny release of any unrelated matters as well as all information protected under the F.O.I.A. and the Federal Privacy Act.

Admissibility at Trial

The Federal Rules of Evidence and judicial determination govern admissibility at trial. The rules are also instructive when considering, and arguing, whether discovery demands are reasonably calculated to obtain admissible evidence.

Under Rule 404(b), "[e]vidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show action in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity or absence of mistake or accident."[34]

The application of Rule 404(b) requires a two-part analysis: first, whether the proposed evidence fits within one of the exceptions provided by the Rule, and, second, even if it does, whether under Rule 403 the evidence's probative value is substantially outweighed by the potential for jury confusion or prejudice.[35]

Courts frequently hold divergent views on the admissibility of prior similar act evidence.[36]

The Second Circuit has upheld the exclusion of evidence of prior unsubstantiated civilian complaints against police officers charged with use of excessive force.[37]

At issue in *Berkovich v. Hicks* was discovery of seven complaints. The Circuit Court found that the fact that defendant had been largely exonerated on all of the charges in prior complaints lessened significantly the probative value of the complaints.[38]

The decision questioned whether plaintiff would have been able to even prove that these incidents occurred, noting that "[s]imilar act evidence is relevant only if the jury can reasonably conclude that the act occurred and that the defendant was the actor."[39]

---

[31] *Id*. at *4.
[32] Harper, *supra* Note 27 at *3.
[33] King, *supra* Note 6 at 191 (the privacy interest in this type of record is not substantial because it is not the kind of "personal" information warranting constitutional protection).
[34] Fed. R. Evidence 404(b).
[35] Shaw v. City of New York, 95 Civ. 9325, U.S. Dist. LEXIS 4901, at *16-17 (S.D.N.Y. Apr. 15, 1997)(citing Rule 404(b) advisory notes).
[36] *See e.g*., O'Neill v. Krzeminski, 839 F.2d 9, 11 (2d Cir. 1988)(noting that panel members held different views on admissibility of prior similar act evidence).
[37] Berkovich v. Hicks, 922 F.2d 1018, 1022-23 (2d Cir. 1991).
[38] *Id.*
[39] *Id.*

Most importantly, the Second Circuit concluded that "it seems improbable that full discovery of the (unsubstantiated) complaints would have led to admissible evidence."[40] The Second Circuit upheld the district court's decision to exclude "any reference to the complaints during the trial under Fed. R. Evid. 403 and Fed. R. Evid. 404(b)" finding that full discovery of the unsubstantiated civilian complaints would not have resulted in a different trial decision.[41]

Properly so, since documents like the CCRB reports do not show "motive, opportunity, intent or the like," but, instead and impermissibly, serve to support argument that, because the defendant was previously investigated for a complaint such as excessive force, the fact-finder should believe plaintiff over defendant. This is the very use of evidence that Fed. R. Evid. 406 is designed to prevent."[42]

The Official Information Privilege and the Freedom of Information Act

As noted above, the Official Information Privilege has been recognized in the absence of a statutory foundation.[43] Its purpose is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation.[44]

While the focus of the law enforcement privilege is to protect information relating to investigations, it is the privacy of police officers involved in an investigation that must be protected, and this privilege does not extend to the privacy of police officers generally. Thus, for example, personnel records of police officers not involved in a particular investigation would not necessarily be privileged unless either a threat to their safety or an interference with the investigation can be shown.[45] Any invocation of the law enforcement privilege must accordingly be accompanied by a specification as to what present or future investigations may be jeopardized by the production of the documents in question.[46] The law enforcement privilege is incorporated within the F.O.I.A.

Under the federal law, records or information compiled for law enforcement purposes are exempted to the extent that disclosure could lead to one or more of six enumerated harms: (a) interference with enforcement proceedings; (b) deprivation of a right to a fair trial or impartial adjudication; (c) an unwarranted invasion of personal privacy; (d) disclosure of the identity of a confidential source; (e) disclosure of techniques and procedures for law enforcement investigations and procedures; and (f) endangerment of the life or physical safety of any individual.[47]

Although the law enforcement exemption originally provided broad protection to "investigatory files," the current language largely comes from a 1974 amendment designed to provide wider public access.[48]

Similarly, every state has its own freedom of information or "right-to-know" laws to provide public access to information at the local level. While they vary from state to state, these laws are similar to the FOIA in that they employ the same general premise and share the same goals.[49]

---

[40] *Id.*
[41] *Id.*
[42] Shaw, *supra*. Note 13 at *17-18.
[43] *In re Dept. of Investigation of the City of New York*, 856 F.2d 481 (2d Cir. 1988).
[44] *Id.* at 484.
[45] Morrissey v. City of New York, 171 F.R.D. 88, 91 (S.D.N.Y. 1997).
[46] *Id*; *see also* Borchers v. Commercial Union Assur. Co., 874 F.Supp. 78, 80 (S.D.N.Y. 1995); Black v. Sheridan Corp. of America, 564 F.2d 531, 546 (D.C. Cir. 1977).
[47] 5 U.S.C. 552(G)(b)(7)(a)-(f)(1994).
[48] Weisberg v. Department of Justice, 489 F.2d 1195, 1197 (D.C.Cir. 1977).
[49] The federal act also allows public access to state and local law enforcement material held by federal

Federal Privacy Act

Police officers have a legitimate privacy interest in the portions of police department files concerning their off-duty, private conduct.[50] This applies directly to medical records.

In 1996, Congress enacted The Healthcare Insurance Portability and Accountability Act (HIPAA) to further the federal goals of increased access to health care and to improve the efficiency and effectiveness of the health care system.[51]

During the legislative process, individual privacy became an increasing concern due to innovations in technology with respect to information sharing.[52] To address these concerns, Congress delegated the Secretary of the Department of Health and Human Services (DHHS) the task of adopting national standards "to ensure the integrity and confidentiality of the information."[53] Pursuant to this congressional mandate, the DHHS implemented its Privacy Rule in 2003.[54] The Privacy Rule controls the "uses and disclosures of protected health information" by "covered entities."[55] Covered entities, including health care providers such as treating physicians, must develop policies, implement procedures, and maintain compliance with the Privacy Rule to ensure against unauthorized disclosure of protected health information.[56] Without such compliance, they face penalties in the form of fines and even imprisonment.[57] The Privacy Rule authorizes a covered entity to disclose protected health information under an enumerated set of circumstances.[58]

As relevant here, disclosure is permitted pursuant to and in compliance with a valid authorization as executed by the patient.[59]

However, a patient's authorization is not necessary if the covered entity is disclosing protected health information in response to a court order, a subpoena, a discovery request, or "other lawful process."[60]

If a subpoena or discovery request is not accompanied by an order of the court, the covered entity must receive "satisfactory assurances" from the party seeking the information that (1) reasonable efforts have been made to ensure that the individual who is the subject of the information has been notified of the request or, (2) reasonable efforts have been made to secure a qualified protective order for the information.[61] If these assurances are not given, the health care entity must itself make reasonable efforts to provide notice or to seek a qualified protective order.[62]

In cases where attempts are made to obtain records without court order and defendant is made aware of the subpoena by the health care entity, defendant must seek a protective order from the court.

Conclusion

While discovery is broadly permitted in federal court actions, defendants have several objections to assert and must be do so in order to protect personal privacy and the integrity of police investigations.

In camera review can be an effective tool to limit discovery of generally permissible documents by requiring plaintiff to set forth what they expect to find

---

agencies. Wojczak v. Department of Justice, 548 F.Supp. 143, 148 (E.D.Pa. 1982).

[50] King, *supra* Note 6 at 191 (the privacy interest in "personal" information warrants protection).

[51] Pub. L. No. 104-191, 110 Stat, 1936.

[52] White, Tamela J. & Hoffman, Charlotte A., The Privacy Standards Under the Health Insurance Portability and Accountability Act: A Practical Guide to Promote order and Avoid Potential Chaos, 106 W.Va. L. Rev. 709, 712-4 (2004).

[53] 42 U.S.C. 1320d-2(d)(2)(A); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82, 465.

[54] 45 CFR Parts 160 and 164.

[55] 45 CFR 164.502.

[56] 45 CFR 164.530.

[57] 42 U.S.C. 1320d-5 and 1320d-6.

[58] 45 CFR 164.502

[59] 45 CFR 164.502 (a)(1)(iv) and 164.508.

[60] 45 CFR 164.512 (e)(1)(i) and (ii).

[61] 45 CFR 164.512(e).

[62] Id.

through a review of the records and how it relates to the subject litigation.

Even where materials are disclosed, if the matter proceeds to trial, defendants must act to limit the use of sensitive information in violation of Fed. R. Evid. 403, 404 and 406.

Finally, the use of a protective order can limit the risk that permissible discovery may leak matters of personal privacy or police investigation to unrelated parties.

What is a "Related" Medical Condition? Pitting the Privacy Interest in Medical Treatment Against the Right to Discover Relevant Evidence

By: Magistrate Judge Terence P. Kemp

Magistrate Judge Terence P. Kemp was first appointed to his position in the Southern District of Ohio in 1987. He is a graduate of the University of Virginia School of Law and Brown University. From 1977-1979, Judge Kemp served as a law clerk to the Honorable Malcolm Muir in the United States District Court for the Middle District of Pennsylvania.

I. Introduction

An employee is fired or demoted for what he or she believes to be discriminatory reasons. A person suffers injuries in a vehicle accident or is harmed by an allegedly defective product. An individual is arrested and charged on allegedly false pretenses and is subjected to an amount of force that the individual claims is both excessive and injurious. These are typical backdrops for litigation in which compensation is sought for both physical injury and emotional distress.

Once the suit is filed and discovery begins, the defendant learns that the injured party has a history of treatment for various illnesses, injuries, or psychological conditions that predate the event that precipitated litigation. Sometimes that treatment is ongoing. Sometimes it encompasses new conditions that have arisen since the case was filed.

Any diligent defense attorney will want to review the plaintiff's entire medical history. Certainly, the defendant needs to know the extent, and cost, of treatment given for the injury allegedly caused by the defendant's acts or omissions. But the possibility also exists that any new injury allegedly caused by the defendant may overlap a pre-existing medical condition, or may be the type of injury that causes symptoms similar or identical to those already being experienced by the plaintiff due to conditions not caused by the defendant's acts or omissions. If so, the defendant will want to argue (with facts derived from the plaintiff's medical treatment records) that any damage award should be limited to the extent of exacerbation of a pre-existing condition or any symptoms not otherwise explained by plaintiff's pre-existing or contemporaneous medical history.

In concept, the need for defendant to go beyond the history of plaintiff's treatment for the precise injury at issue in the case is not controversial. The difficulty arises, however, in putting the concept into practice. For various reasons, an injured plaintiff is not usually willing to give the defendant a blanket release to obtain the plaintiff's entire medical history from birth forward. Even if the history is unremarkable, most people feel (and society generally supports that feeling) that their medical history is no one's business but their own. Further, the need for confidentiality in the relationship between patient and physician (or other health care provider) is important, if not essential, to the ultimate goal of correct treatment. If the patient withholds information from the provider out of concern that it will be publicly disseminated, the provider may not be able to diagnose and treat the actual condition being experienced by the patient. This need for privacy in the medical treatment context is recognized by a variety of state and federal statutes, rules of evidence, and court decisions which not only proscribe the discovery and use of

certain medical records as evidence, but which impose civil or criminal penalties for their unauthorized disclosure.

Thus, the dilemma arises. Plaintiffs understand that by seeking compensation for an injury, they have effected a limited waiver of their medical privacy. Defendants from whom such compensation is sought would ideally like to review the entirety of the plaintiff's medical history to explore any conceivable connection between the present injury or condition and any other injury or condition which cannot be attributed to their acts or omissions. To complicate the matter further, they are forced to request such records without advance knowledge of what might be in them, making their arguments in favor of disclosure somewhat abstract (e.g. if the plaintiff alleges emotional distress due to sex discrimination, records of a prior psychological condition - or even reports to a treating health care provider of other stressors in the plaintiff's life - *may* be relevant to that claim). Without knowing the type of pre-existing condition, however (*e.g.* is it a bipolar disorder or just a report of occasional anxiety), when it occurred, what symptoms it caused, how it responded to treatment, and whether the situation which caused it has now resolved, it is hard for defendants to make intelligent arguments, or the court to make informed decisions, about how broad a waiver of the plaintiff's privacy interests ought to be enforced.

The court stands as the final arbiter in this clash between an injured party's privacy interests and a defendant's right fairly to defend its financial interests. The court must make two types of decisions, both of which have ramifications for each party's interests: (1) what is the substantive legal standard to apply, and (2) what types of procedures will maximize the chances that each party's interest is adequately addressed. These decisions are not made on a blank slate, but are informed by applicable rules of procedure, evidence codes, state and federal statutes, and other court decisions. This article will review these various sources of procedural and substantive law in an attempt to shed light on the types of frameworks for decision-making that have been adopted by the courts in response to this real-world dilemma, and how the choice of a framework and substantive legal standard might operate to produce an appropriate judicial resolution of the problem.

II. The Importance of Medical Privacy

The issues raised by an effort to discover evidence about a litigant's medical history would not be as difficult or sensitive if the only question presented was relevance. Rules of procedure typically permit the discovery of some arguably irrelevant evidence in order to streamline pretrial proceedings, based in part on the concept that such discovery does not ordinarily harm the party disclosing the evidence beyond the time and expense that may be spent on irrelevant matters. So, for example, Federal Rule of Civil Procedure (Fed.R.Civ.P.) 30(d)(1) allows relevance objections to be made during a deposition, but contemplates that the arguably irrelevant testimony is still given, subject to the objection, unless a claim of privilege is being made.

The unwarranted disclosure of medical evidence, however, is not seen as a matter of mere inconvenience. Although the right to non-disclosure of medical information has not been elevated to the status of a federal constitutional right [1. See, e.g., *Doe v. Wigginton*, 21 F. 3d 733 (6th Cir. 1994).], and the federal courts do not generally recognize a physician-patient privilege [2. See *Whalen v. Roe*, 429 U.S. 589, 602 n. 28(1977)], some aspects of the health care provider relationship, such as statements made to a psychotherapist during the course of treatment, are subject to a federal common-law privilege against disclosure. [3. See *Jaffee v. Redmond*, 581 U.S. 1, 11 (1996), which characterizes "[t]he mental health of our citizenry" as a

"public good of transcendent importance."] Federal statutory law, on the other hand, evinces a strong concern for the confidentiality of patient information. [4. *See, e.g.,* the Health Insurance Portability Protection Act (HIPPA), which provides, in 42 USCA § 1320d-6, for criminal penalties, including fines and imprisonment, for anyone who obtains or discloses "individually identifiable health information" (i.e. information provided to a health care provider about the physical or mental health of an individual) unless such disclosure is authorized under the Act.] Federal courts have used this clear statement of Congressional policy, as well as the well-accepted notion that "[b]y their very nature, records of medical and psychological treatment are inherently private" [5. Fischer v. City of Portland, 2003 WL 23537981, *4 (D. Ore. August 22, 2003)] to engage in an analysis of the discoverability of medical evidence that is similar to that used in considering a claim of physician-patient privilege under state law.

States, of course, have almost uniformly recognized an evidentiary privilege shielding discovery or disclosure of medical evidence absent a waiver by the patient. [6. Ohio Revised Code §2317.02, which prohibits the introduction of testimony from "[a] physician or a dentist concerning a communication made to the physician or dentist by a patient in that relation or the physician's or dentist's advice to a patient" absent a waiver by the patient or unless one of a number of statutory exceptions apply, is typical of such state privilege laws.] The state-created privacy interest in medical information typically extends beyond a mere evidentiary privilege; many states allow a patient to sue a heath care provider for damages for disclosing such information without the patient's consent. [7. See, e.g., *Biddle v. Warren Gen. Hosp.*

86 Ohio St.3d 395, 715 N.E.2d 518 (1999), recognizing "an independent tort ... for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship."] Again, such laws recognize both the public interest served by the provision of adequate health care to patients based upon a full and complete report of symptoms, and the private interest in keeping such information out of the public domain.

The public is generally concerned about any effort to dilute the protection available for medical records, even if the purpose of such efforts is to improve the quality of health care. Thus, for example, bills proposed in both the House and Senate which would create a nationwide electronic database of medical records that could be accessed by medical providers at any location - and which would greatly enhance the ability of such providers to care for patients who are unable to provide a medical history or whose primary treatment occurred in another location - have been opposed on grounds that they do not adequately protect the privacy of such records. [8. For a discussion of this issue, See, e.g. http://www.patientprivacyrights. org, (accessed on January 4, 2007) discussing H.R. 4157 and S. 1418, two proposals dealing with the nationwide electronic medical record network, and describing one portion of the bills as "a disaster for privacy."] Given this background, it is not surprising that significant tension is created by a defendant's request for a plaintiff's medical history, even if the failure to comply with a legitimate request for medical records may jeopardize the plaintiff's ability to recover damages for injuries suffered at the hand of the defendant. This tension frequently spills over into concrete disputes about the proper scope of medical discovery in cases where a personal injury is alleged and makes the courts the final arbiter of the extent to which the plaintiff's medical records may be reviewed by the opposing party and ultimately disseminated in public.

III. The Procedural Framework

Modern-day litigators take for granted the concept that a party who is sued for damages has an almost unfettered right to discover any and all information that will enable it to defend fairly and fully its financial interests. Although there have been some limitations added in recent years to the rules governing discovery, it is still generally true (at least in the federal courts) that a party has the right to ask for, and to receive, any information that is "relevant to the claim or defense of any party" and, upon a showing of good cause, additional information that is "relevant to the subject matter involved in the action." [9. Fed.R.Civ.P. 26(b)(1).] Such litigants are also entitled to have an injured party submit to an examination by a health care provider chosen by that party's opponent if the injured party has placed his or her physical or mental condition "in controversy." [10. Fed.R.Civ.P. 35(a).]

On the other hand, the scope of discovery is limited by the presence of the words "not privileged" appearing immediately before Rule 26(b)(1)'s broad description of the type of discovery which is otherwise available in federal litigation. Further, Fed.R.Civ.P. 26(c) allows the Court to restrict or even prohibit discovery that would cause a litigant to experience "annoyance, embarrassment, oppression, or undue burden or expense," and Rule 26(b)(2) permits the Court to act similarly if "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." Thus, the federal courts are given a measure of discretion to deny a request to discover even irrefutably relevant evidence if other factors make the request for such evidence unduly burdensome, oppressive, or otherwise unreasonable.

In any litigation commenced in a state court, that state's privilege laws will generally come into play when medical records are being sought. In litigation in federal court, if the case arises under state law, the privilege law of that state is made applicable by Federal Rule of Evidence 501. If the case arises under federal law, federal privilege law applies, and the federal courts will also be required to perform the balancing required by the provisions of Fed.R.Civ.P. 26 cited above. Thus, disputes about medical records will be presented to a court that is already predisposed to weigh the privacy interests of the injured party against the need of the opposing party for a full and complete disclosure of information needed to defend itself against a claim for money damages. As in any such situation, the challenge for the court is not so much the articulation of general rules for decision-making, but the application of those general (and competing) rules to particular situations where it is less than crystal clear which of the two competing interest should prevail.

IV. How the Courts Decide Medical Privacy Issues

The beginning of any inquiry into the discoverable nature of medical records is whether those records are relevant to the plaintiff's claim of compensable injury. Relevance is a broad concept. For trial purposes, relevant evidence is defined (at least in the federal court system) as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable that it would be without the evidence." [11. Federal Rule of Evidence 401.] Relevance for discovery purposes is even broader, consisting of both any facts that are relevant under Fed.R.Evid. 401 and any other information "reasonably calculated to lead to the discovery of admissible evidence." [12. Fed.R.Civ.P. 26(b)(1).] Consequently, before the court is required to engage in any

weighing of the defendant's need for medical evidence and the plaintiff's desire not to disclose any more such information than is necessary, the court must make a threshold decision about how much medical information is arguably relevant and discoverable.

Again, due to the policy favoring broad discovery in civil litigation, courts have defined relevant medical evidence in broad terms. A typical formulation is to deem any medical record relevant to a claim of injury if it either describes treatment given for the claimed injury or "shed[s] light on other contributing causes" of that injury. [13. *Walker v. Northwest Airlines Corp*., 2002 WL 32539635, *3 (D.Minn. October 28, 2002). It is important to note, however, that some courts have identified as a threshold issue, in cases involving claims of emotional distress, whether the plaintiff alleges only "garden variety" emotional distress or a more serious psychological condition that will be supported by testimony or records from a mental health care provider. According to those courts, allegations of "garden variety" emotional distress do not place the plaintiff's mental condition "in controversy" and a defendant's request for treatment records relating to the plaintiff's overall mental condition are deemed to be either irrelevant or of such marginal relevance that they are not discoverable. For an extended discussion of the different approaches which courts have taken to this issue, and the related issue of whether an allegation of "garden variety" emotional distress waives the federally-recognized patient-psychotherapist privilege, See *Miles v. Century 21 Real Estate LLC*, 2006 WL 2711534 (E.D.Ark. Sept. 21, 2006); and compare with Jarick v. City of New York, 2006 WL 1379585 (S.D.N.Y. May 18, 2006) (noting that if a plaintiff makes "allegations of serious, specific psychiatric injuries for which the plaintiff sought and received treatment ... the details of her prior treatments are highly relevant, and the plaintiff cannot pick and choose which stressors she will reveal and which she will redact."] The first difficult substantive question thus entails making a determination of the relationship between an injury and events in the injured party's medical history which might either be other "contributing causes" to the claimed injury or which might "shed light" on such causes.

As one might imagine, answering that question involves not only some measure of legal analysis, but a factual inquiry into issues of actual or potential medical causation. Some of the medical issues may be straightforward, allowing the court to rely upon common-sense assumptions about the relatedness of medical conditions (for example, it would seem reasonable to conclude that treatment for a prior and now-resolved case of athlete's foot would be unrelated to claim for damages arising from a broken arm suffered in an automobile accident). Others are more complex, especially in the area of emotional or psychological injuries, which can be related to conditions that either manifest themselves as early as childhood, or which stem from events going far back in time even if the manifestation of the illness is more recent.

In the latter context, most courts have acknowledged the general principle that records of prior psychological treatment are "relevant as to both causation and the extent of plaintiff's alleged injuries and damages if plaintiff claims damages for emotional pain, suffering, and mental anguish." [14. *Owens v. Sprint/United Management Co.*, 221 F.R.D. 657, 659 (D.Kan.,2004).] Some courts have chosen to deal with these types of issues by limiting discovery to a specific time frame around the events that led to litigation [15. For example, in *Garrett v. Sprint PCS*, 2002 WL 181364 (D.Kan., January 31, 2002), the court limited discovery of records of psychological treatment to those pre-dating the alleged discrimination by three years, thus concluding implicitly either that earlier records were irrelevant or that a balancing of factors precluded discovery of those

earlier records.], while others have apparently permitted defendants to go back much further in time. [16. See *Moore v. Chertoff*, 2006 WL 1442447 (D.D.C., May 22, 2006) (granting motion to compel plaintiff to execute medical releases for records of psychological treatment for the past ten years).] Logically, it would appear that the temporal proximity of the records to the event in question in the litigation is only one of many factors that touch upon the relevancy of the records, so the issue of how recent or remote such records may be should not ultimately be dispositive on the issue of how far back (or forward) a defendant is permitted to go during discovery.

A number of courts, recognizing the problems inherent in any categorical approach to such records, and also recognizing the difficulty presented when a court is asked to make judgments about medical causation in the absence of a fully-developed record, have placed the burden on the injured party to demonstrate that the requested medical records are irrelevant to his or her claim of injury. [17. See, e.g., *Merrill v. Waffle House, Inc.*, 227 F.R.D. 467, 473-74 (N.D. Tex.,2005)("The Court recognizes that all medical records, and especially records pertaining to treatment for purely physical conditions, will not necessarily be relevant to mental anguish claims. However, it is Plaintiffs' burden to establish that show that there [is] 'no possibility' that the requested records may be relevant to the claim or defense of any party or are of 'such marginal relevance that the potential harm occasioned by discovery would outweigh the ordinary presumption in favor of broad disclosure,'" quoting *Scott v. Leavenworth Unified School Dist. No. 453.*, 190 F.R.D. 583, 585 (D.Kan.,1999).] Under this approach, the injured party is required to collect and submit the records to the court for an *in camera* review, and the failure to do so results automatically in an order that the records be provided to the opposing party. Although the tactic of placing the burden of demonstrating irrelevancy on the injured party forces the party with the greater access to information to move the inquiry forward by assembling and submitting records, it does not necessarily assist the court in deciding the relevance of those records once they have been submitted for review.

An alternate approach, of course, is to place the burden of demonstrating relevance on the requesting party. That is problematic, however, because that party does not have any knowledge of what might be in the plaintiff's medical records, and is therefore limited in the types of arguments that can be made in support of disclosure. Some courts have implicitly adopted this approach, however, and have denied requests for records whose contents are unknown on grounds that the relationship between those records and the plaintiff's present condition is simply "speculative." [18. See, e.g., *Pasternak v. Texaco Inc.*, 1997 WL 621267, *1 (S.D.N.Y. October 7, 1997) ("Defendants' argument that they are nonetheless entitled to production of all other medical records simply because of the remote possibility-unsupported by any evidentiary showing whatever-that one or both plaintiffs may have at some uncertain time in the past suffered some unknown physical injury that might conceivably create a basis for arguing that such plaintiff had a latent pre-existing psychological injury -is blatantly speculative, personally intrusive, and was well within the discretion of the Magistrate Judge to deny."]

In an effort to reach a middle ground, some courts have attempted to create categorical descriptions of what types of records are relevant and what types are not. For example, in a case where a physical injury resulting in continuing disability is alleged, courts may limit discovery to records concerning related conditions (i.e. other back injuries suffered by the plaintiff when the injury at issue is a herniated disc) or those which concern unrelated injuries which were either permanent or are ongoing. The former types of records are relevant because they shed light on "the

injury in issue" while the latter "are relevant to the jury's assessment of the extent of the loss of enjoyment of life attributable to the accident." [19. *Moreno v. Empire City Subway Co.* Slip Copy, 2006 WL 2053191, *1 (S.D.N.Y. July 21, 2006).] Such conditions are contrasted with "transitory conditions" which are both dissimilar to the current injury and which have resolved prior to the occurrence of that injury. ["Examples of transitory conditions that would be irrelevant include a simple fracture that heals without complications or a respiratory infection that runs its course without sequelae." *Id.* at n. 2.] Using this approach allows a defendant to identify relevant categories of records, thus lessening the chance that the request will be deemed "speculative," while at the same time providing some guidance to the plaintiff as to what types of records must be produced and what may properly be withheld. Presumably, under this approach, although the defendant would be permitted to subpoena relevant records, it would still be the injured party, in conjunction with the treating health care provider, who would screen the larger universe of past medical records to determine what records, or portions thereof, are responsive to the request.

In an ideal world, where time and information constraints are non-existent, a much more precise approach could be taken which would always strike the appropriate balance between the injured party's right to privacy and the defending party's need to gather information which is fairly related to its defense. Issues of medical causation and medical relatedness would be made on the basis of medical evidence and expertise, and there would be little risk either that an injured party would withhold evidence just because the contents of the withheld records would not be subjected to scrutiny by the courts, or that a defending party would obtain evidence of little probative value but carrying a large potential for embarrassing or humiliating the injured party and then use the threat of disclosure of that evidence as leverage in the litigation. That is not the real world of litigation, however, where decisions about discovery are often made in a compressed time frame and, for reasons related both to time and resources, based on little or no input from health care professionals. Thus, questions concerning medical relatedness are usually dissected with blunt instruments rather than with laser-like precision.

V. Conclusion

Medical privacy is an important issue both to the public at large and to individuals who seek medical treatment with the legitimate expectation that the number of persons who learn of their maladies, symptoms, and treatment will be strictly limited. When such a person is injured, through no fault of his or her own, under circumstances where another may be legally liable for that injury, it seems harsh to require the innocent injured party to give up some or all of his or her medical privacy in order to recover just compensation for the injury. On the other hand, allegations of causation, injury, and disability cannot simply be taken at face value, and as long as there is an adversary system in place for deciding disputed questions of fact, the party from whom compensation is sought has a right to contest any claim of compensation, and the public has a right to know that such claims are resolved in manner that is fair to both parties and based upon real evidence.

As usual, when such public and private interests are in tension, courts are tasked with resolving that tension by balancing the interests and finding some middle ground. They have attempted to fashion rules which allow the parties to make preliminary predictions about how much of each party's interest will be accommodated, but the fact-specific nature of the required balancing of interests leaves many parties dependent upon the courts to strike the appropriate compromises. Hopefully, courts will retain

the flexibility to adopt decisional rules and procedural approaches that provide the parties and the public with at least "rough justice" and which make possible some level of individualized decision-making without causing the litigation process itself to break down. It is certain that, in any case, a court may be legitimately criticized for forcing too much, or permitting too little, disclosure of medical information, but there should be little room to dispute that the courts as a whole make a genuine effort to recognize and protect the right of medical privacy and limit intrusions to those that are necessary in order to preserve both private and public confidence in the integrity of the process through which parties who are subjected to claims for money damages are ultimately held responsible for the injuries they have caused - and only the injuries they have caused.

The ideal approach to this issue is to make an individualized assessment in each case, eschewing any formalistic burden-shifting or categorical approaches in favor of a careful analysis of the type of injury alleged and the types of past or concurrent conditions that are reasonably likely to be relevant to the cause or impact of the injury. That may, in some cases, require the Court to conduct an *in camera* review of records, although that can and should be reserved for those exceptional cases in which no other approach will be satisfactory. More often, the Court should recognize the problems presented by unequal access to the exact details of the injured party's medical records and encourage, or even order, the parties to allow either defense counsel or an expert to have access to the records for purposes of making an initial evaluation of relevance and assembling information to argue the point. Once the playing field has been leveled, the requesting party should still have to satisfy the obligation imposed by the pertinent civil rule to make a sufficient showing of relevance that will overcome the privacy interests involved. While potentially more time-consuming than categorical approaches, this kind of procedure (especially if it becomes widely accepted among the litigants in a particular jurisdiction) should ultimately result both in better decisions and less contentiousness about whether particular medical records are discoverable or whether the injured party's privacy interest will prevail.

The Privacy Project III

Privacy in the Executive Suite: The Apex Doctrine

By: Ralph Streza and Patrick T. Lewis

Few things strike at the nerves of in-house counsel more effectively than a notice of a deposition of the CEO or Chairman of the Board of Directors, especially when the potential deponent has minimal or no knowledge of relevant information. All too frequently, outside counsel understate the impact of the deposition of a corporate executive: outside counsel may view that deposition notice as a relatively minor event by virtue of the executive's likely limited knowledge of the facts. But depositions of high-ranking executives are very disruptive to the executive's business and raise several public relations and privacy-driven concerns that may not be obvious to outside counsel. Except in cases where high-ranking depositions form part of the proposed deponent's corporation's discovery plan, the noticed deponent and in-house counsel will probably want to prevent the deposition from going forward or, failing that, will want significant restrictions placed on the deposition.

In many instances, the deposition notice may be intended to harass the corporate or government opponent into settlement considerations. In other instances, the high ranking official may actually have discoverable information. In even other instances, the official's deposition may be irrelevant to the actual facts of the case, but relevant to a corporation's particular motivation or intention. The Apex Doctrine serves to put controls on the scope of the deposition or in most situations, stop the deposition from occurring.

While the Federal Rules of Civil Procedure and the counterpart state rules do not expressly recognize a corporate privacy interest at stake, the judicially created, and in some states, legislatively recognized Apex Doctrine acts to shield high ranking corporate and government officials from the deposition discovery procedure. A business or governmental entity is entitled to operate in peace and to a very real extent, having its corporate leadership noticed for and participate in deposition discovery distracts the organization from obtaining that goal.[1]

High ranking corporate executives usually are exceptionally busy people who manage many major issues. They tend to be frequent travelers and find it difficult to devote the time to prepare for the deposition, let alone remain focused on the scope of the deposition. Allowing the deposition of those officers in one case serves as precedent to allow a deposition in the next case, thereby increasing the risk that giving deposition testimony becomes part of any official's job description. The Apex Doctrine is intended to allow an executive's deposition only in exceptional circumstances.

IADC member Ralph Streza is of counsel with Critchfield, Critchfield & Johnston, Ltd. in Medina, Ohio, which he joined in July 2007. His practice has focused on defending corporations in complex commercial and product liability litigation. He attended Cleveland-Marshall College of Law, and graduated cum laude in 1982.

Patrick T. Lewis is a litigator resident in the Cleveland, Ohio office of Porter Wright Morris & Arthur. He earned his law degree cum laude from Harvard Law School in 2004 and an A.B. summa cum laude from the College of William & Mary in 2000.

[1] *See* Cincinnati v. Correll, 141 Ohio St. 535, 540, 49 N.E.2d 412, 415 (1943) (noting that "the right to carry on … business is a property right constitutionally protected against unwarranted and arbitrary interference").

The Apex Doctrine is not an absolute blanket. It is not an immutable rule that protects high ranking officials from a deposition in every case; indeed, whether and to what extent the Apex Doctrine applies involves a fact-specific analysis. Moreover, there are judicial officers who believe that the a litigant's right to liberal discovery trumps the Apex Doctrine. Fortunately, for those cases, counsel have access to writs of prohibition and other extraordinary appellate relief to install controls on or stop the deposition.[2]

While discovery generally and depositions specifically are intended to invade the privacy interest of the opposing litigant and to eliminate secrecy in trial preparation, the Apex Doctrine is intended to preserve corporate or governmental privacy while recognizing on the other hand, that litigants are entitled to having all relevant facts revealed in the search for truth and resolution of judicial disputes.

The article will focus on and analyze the legal foundations and trends for the Apex Doctrine in order to provide a concise reference for use in responding to a deposition notice of a high ranking official, with citations to some of the leading cases and outcomes.

What Is The Apex Doctrine?

The Apex Doctrine is, for the most part, a judicially created doctrine that imposes special burdens on a party seeking to take the depositions of so-called "apex" employees. One of the first Apex Doctrine cases was an admiralty case in the Southern District of New York. The case, *Porazzi Co. v. Mormaclark*, involved a claim pertaining to certain shipments.[3] The libellant noticed the deposition of the shipping company's Vice President, General Claims Agent, and the Master and Chief Mate of the vessel, to testify concerning documents and matters about the shipments. The company objected on the grounds that the Vice President had no personal knowledge of the shipments, and his production would be an annoyance, embarrassing, and oppressive. The court agreed that the deposition of the Vice President was improper because "the Vice President could contribute nothing beyond that which could be gleaned from an examination of the General Claims Agent."[4] While the *Porazzi* court did not use the term "apex" to describe the Vice President, that term evolved over time.

Courts use various nomenclatures for "apex" employees: "high level corporate executives," "top-level decision-makers," and "high-level corporate official" are among the terms employed by courts applying the doctrine.[5] While the Apex Doctrine is focused on "corporate" executives, courts have applied it to heads of government and agencies within government.[6]

There is no clear definition of how "high" a high-level official must be for the Apex Doctrine to apply. While most cases interpreting the doctrine have focused on efforts to depose CEOs, some have also applied the doctrine to senior vice presidents and division-level presidents.[7] Suffice to say, where a deposition notice of

---

[2] *See, e.g.*, In re Alcatel, 11 S.W.3d 173 (Tex. 2000), where the corporate defendant successfully obtained a writ of mandamus by invoking the Apex Doctrine in the Texas appellate court and upheld by the Texas Supreme Court, discussed infra.

[3] 16 F.R.D. 383 (S.D.N.Y. 1951).

[4] *Id.*

[5] *See, e.g., Folwell v. Hernandez*, 210 F.R.D. 169, 173-74 (M.D.N.C. 2002); Baine v. General Motors Corp., 141 F.R.D. 332 (M.D. Ala. 1991); State ex rel. Ford Motor Co. v. Messina, 71 S.W.3d 602 (Mo. 2002); Crown Central Petroleum Corp. v. Garcia, 904 S.W.2d 125 (Tex. 1995); Thomas v. International Bus. Mach., 48 F.3d 478, 483 (10th Cir. 1995).

[6] *See* Rinaldi v Livonia, 69 Mich. App. 58, 69-72, 244 N.W.2d 609 (1976) (barring deposition of senior police and civil officials where their testimony was of minimal relevance and where facts could be determined in less obtrusive ways).

[7] *See* Evans v. Allstate Ins. Co., 216 F.R.D. 515 (N.D. Okla. 2003) (protecting CEO and senior VP from deposition); Folwell, *supra* n. 2 (protecting divisional CEO from deposition).

a high ranking official has been noticed, counsel should consider the assertion of the doctrine.

Once a potential deponent is subject to the Apex Doctrine, the party seeking to bar the deposition typically need only produce an affidavit from the targeted executive stating that the executive lacks personal knowledge of the facts in dispute.[8] In some circumstances, the Apex Doctrine can be triggered when the targeted executive has substantial relevant knowledge about the facts of the case.[9] When the Apex Doctrine is triggered, the burden shifts to the party seeking to take the deposition to show that they cannot obtain the needed discovery from less burdensome sources, such as through a corporate designee or a lower-ranking employee, [10] or through written discovery. [11]

Authority For The Apex Doctrine

The judicial authority for the Apex Doctrine varies by jurisdiction, as there is no explicit reference to the Apex Doctrine within the text of the Federal Rules of Civil Procedure or the rules of most states. In most cases, the doctrine is essentially common law and derives from the general power of the judiciary to control the discovery process. However, in some instances, "apex" deposition procedures are set forth in local rules.

The Apex Doctrine's foundation comes from implications of the discovery rules – particularly Fed. R. Civ. P. ("Rule") 30(a)(1) and 26. Parties seeking to take the deposition of corporate executives frequently employ Rule 30(a)(1) to do so. Rule 30(a)(1) allows the deposition of "any person" – which includes corporate officers and agents and government officials. However, in the 1970 amendments to the Federal Rules, Rule 30(b)(6) was adopted to solve a procedural problem and to place the onus on corporations to designate their employees and officers who are most knowledgeable on subjects to testify on behalf of the corporation.[12] Parties seeking to depose "apex" employees, however, will frequently utilize the Rule 30(a)(1) process to notice "apex" depositions.[13]

Mechanically, when an "apex" employee is noticed for deposition, the corporation must file a motion for a protective order to stop or control the deposition. Rule 26(b)(1) permits parties to "obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party." However, Rule 26(b)(2)(C) sets forth rules limiting a litigant's power to use the discovery process as follows:

> The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is *unreasonably cumulative* or *duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive*; * * * or (iii) *the burden or expense of the proposed discovery outweighs its likely benefit*, taking into account the needs of the case ,the amount in controversy, and

---

[8] *See, e.g.,* Evans, *supra* n. 5, at 519; Harris v. Computer Assocs. Int'l, Inc., 204 F.R.D. 44, 46 (E.D.N.Y. 2001); Thomas, supra n. 3, at 483; Lewelling v. Farmers Ins. of Columbus, Inc., 879 F.2d 212, 218 (6th Cir. 1989).

[9] *See infra* at 6.

[10] *See, e.g.,* Evans, *supra;* Crown Central, *supra* n. 5, at 128 (describing process under Texas law); Salter v. Upjohn Co., 593 F.2d 649, 651 (5th Cir. 1979) (upholding protective order that barred the deposition of the defendant's president in a wrongful death suit because that other employees had more direct knowledge of the facts in dispute).

[11] *See* Mulvey v. Chrysler Corp., 106 F.R.D. 364, 366 (D.R.I. 1985) (requiring party to first explore executive's knowledge through written interrogatories).

[12] *See* Folwell, *supra* n. 5, at 171 (citing 8A Charles Alan Wright, FEDERAL PRACTICE AND PROCEDURE § 2110 (ed. 1994)).

[13] *Id.* at 173.

> the importance of the proposed discovery in resolving the issues.

(emphasis supplied). The Court then has the option to invoke the Apex Doctrine pursuant to the powers granted to it under Rule 26(b)(2).

Some courts have incorporated some or all of the principles underlying the Apex Doctrine into local rules in an effort to set clear boundaries on the process. The Eastern District of New York is one such jurisdiction. Eastern District of New York Rule 30.5 provides:

> (a) Where an officer, director or managing agent of a corporation or a government official is served with a notice of deposition or subpoena regarding a matter about which he or she has no knowledge, he or she may submit reasonably before the date noticed for the deposition an affidavit to the noticing party so stating and identifying a person within the corporation or government entity having knowledge of the subject matter involved in the pending action.
>
> (b) The noticing party may, notwithstanding such affidavit of the noticed witness, proceed with the deposition, subject to the witness's right to seek a protective order.

Rule 30.5 does not appear to fully incorporate the Apex Doctrine. Instead, Rule 30.5 appears to permit a corporate executive noticed for deposition pursuant to either a subpoena or a Rule 30(a)(1) deposition notice to proffer a Rule 30(b)(6) corporate designee to testify as to the pertinent issues. Pursuant to Rule 30.5(b), the noticing party then has the option to accept the Rule 30(b)(6) designee in lieu of the executive, or can proceed with the deposition (which has the effect of causing the corporation to file for a protective order, which involves the court).

Typical Applications of The Apex Doctrine

A. Prevention of Harassment

The most common application of the Apex Doctrine is to prevent the harassment of senior corporate executives by a party seeking to gain settlement leverage, or a party's counsel seeking a feather for their caps. In these situations, the litigant will seek to depose senior corporate executives as an attempt to use harassment and the expense of preparing the executive for deposition for settlement leverage. In articulating the policy rationales behind the Apex Doctrine, courts frequency focus on the need to protect corporations from this particular type of harassment and abuse of the discovery process.[14] In fact, in prohibiting a products liability plaintiff from deposing former Chrysler chairman Lee Iococca, one federal court held that the court had a duty to "recognize his vulnerability" and to take action to prevent litigants from abusing corporate executives through deposition.[15]

One instructive example of a case involving harassment of a senior executive was *Digital Equipment Corp. v. System Indus., Inc.*[16] The case involved a patent dispute; The defendant filed a counterclaim alleging that the patents were "fraudulently obtained" and that the plaintiff brought its

---

[14] *See, e.g.*, Folwell, *supra* n. 5, at 174 (quoting *In re* Bridgestone/Firestone, Inc. Tires Prods. Liab. Litig., 205 F.R.D. 535 (S.D. Ind. 2002) (limiting deposition to avoid the possibility of numerous, repetitive, or harassing depositions)); Messina, *supra* n. 5, at 607 (holding that courts should consider the "burden, expense, annoyance, or oppression to the organization and the proposed deponent" when ruling on discovery motions relating to apex depositions); Hughes v. General Motors Corp., 1974 U.S. Dist. LEXIS 8036 (S.D.N.Y. June 18, 1974) (granting motion for protective order barring deposition of GM's president where "the request borders on harassment and would at best result in a duplication of testimony").

[15] Mulvey, *supra* n. 11, at 366.

[16] 108 F.R.D. 742 (D. Mass. 1986).

complaint knowing that the "patents should never have issued."[17] The defendant then noticed the deposition of the plaintiff's president in an effort to inquire into the plaintiff's motives and reasons for bringing the suit. The plaintiff moved for a protective order barring the deposition on the grounds that the president was exceptionally busy, and that the defendant already deposed those officials with more direct knowledge of the development of the patented technology.[18] The plaintiff's president also provided a declaration stating that he had no recollection of any discussion with respect to the defendant.

The court granted the protective order, holding that the order was necessary to prevent the "harassment and annoyance" of the plaintiff's president. The defendant's attorneys, during an earlier deposition of a less senior employee, stated on the record that "well, you've just guaranteed that we're going to waste one of [the DEC president's] afternoons, also."[19] The court relied on that statement to conclude that it was obligated to protect the executive from a party who made it "transpicuously clear" that it intended to harass that executive.[20] Few cases will probably have such clearly articulated intent to harass as *Digital Equipment*, however, absent a demonstrated effort to depose less senior officials or to discover the relevant information differently, the Apex Doctrine supplies a presumption of a sinister motive.[21]

[17] *Id.* at 743.
[18] *Id.* at 744.
[19] *Id.*
[20] *Id.*
[21] Messina, *supra* n. 5, at 608-09 (noting that plaintiffs' failure to first seek relevant information through "less intrusive means," and considering the same as evidence of harassment); *In re* Burlington N. and Santa Fe Ry. Co., 99 S.W.2d 323, 327 (Tex. App. – Fort Worth 2003) (granting protective order partially on the basis that plaintiffs failed to make a good faith effort to discover the information through less intrusive means).

B. Deponent Has Discoverable Knowledge

In some cases, however, the corporate executive *may* actually have discoverable knowledge. But for most courts, whether the executive has some knowledge does not end the inquiry. Rather, the focus shifts to an analysis of whether the executive's knowledge is "unique" or "superior" regarding relevant facts.[22] While courts do not require the executive to literally be the only person possessing the knowledge in order to be subject to deposition,[23] they do require that the executive's knowledge be at least knowledge not generally known throughout the company. Thus, depositions of apex individuals in products liability cases and other such matters where the apex representative may have, at best, limited knowledge of the facts are routinely disallowed under the Apex Doctrine.[24]

A typical case in which an apex deposition may be allowed is in a contract dispute, antitrust action, or other activity in which the executive was a key player. For example, *Columbia Broadcasting Systems v. Ahern* involved a complex breach of contract action involving the delivery of five record albums to CBS's Records Group.[25] The defendants sought to continue the deposition of CBS's Records

[22] *See, e.g.*, Baine, *supra* n. 5; Mulvey, *supra* n. 11, at 364; Liberty Mut. Ins. Co. v. Superior Court, 13 Cal Rptr. 2d 363 (Cal. Ct. App. 1992); Crown Central, *supra* n. 5, at 125.
[23] *See* Spreadmark, Inc. v. Federated Dep't Stores, Inc., 176 F.R.D. 116, 118 (S.D.N.Y. 1997) (permitting deposition of Federated's chairman and CEO regarding certain contract negotiations even though another Federated representative was present for several of the conversations making up the negotiation).
[24] *See, e.g.*, Evans, *supra* n. 7 (granting protective order stopping the depositions of senior insurance company officials in consumer insurance bad faith litigation); *In re* Burlington, *supra* n. 24 (granting writ of mandamus barring deposition of railroad CEO in personal injury matter); *Messina*, supra n. 5 (barring deposition of Ford executives in products liability case).
[25] 102 F.R.D. 820 (S.D.N.Y. 1984).

Group president, Mr. Yetinkoff, after it had been adjourned after 5 hours due to scheduling issues. CBS objected, arguing that Mr. Yetinkoff's time was very valuable and that the defendants had wasted his time.[26] The court disagreed, ordering that the deposition go forward, because a witness's busy schedule is not an excuse to forego a deposition, and because the president had personal knowledge "not necessarily shared by other CBS employees."[27] The court, however, restricted the deposition to one day's length, and informed CBS that it could seek appropriate relief if the defendants abused the discovery process during his deposition.[28]

Even in these instances, the party seeking the apex deposition must exhaust less intrusive sources of the information.[29] The Apex Doctrine applies even when the targeted executive has discoverable knowledge, but the opposing party has not availed itself of less intrusive means to discover the same information.[30] In that way, parties are not deprived of their discovery rights, but are also not permitted to include senior executives unless it is absolutely necessary to do so. By policing this boundary carefully, counsel for the corporation or the government agency can help protect the privacy of the boardroom from disruptions by the opposing party.

C. Party Seeks To Inquire Into Corporate Motives Through Apex Deposition

Where motive and intent behind corporate action are at issue, there is a strong presumption that the depositions will proceed, but, even the cases that allow apex depositions offer instruction that if the deposition is unreasonably duplicative or cumulative, the deposition may still be sidetracked or reasonable controls placed on the deposition.

When corporate executives are asked to testify about the corporation's "motives," courts applying the Apex Doctrine tend to look to the materiality of the corporation's "motives" in the litigation. In cases where the corporation's motive is of limited relevance, the court may bar the deposition.[31] However, when the motive is a key issue, a court may be more willing to permit the apex deposition to go forward.[32] For example, *General Star Indemnity Co. v. Platinum Indemnity, Ltd.* involved a series of complex commercial and insurance transactions relating to weather-related risks.[33] The issue in the litigation that gave rise to a demand for an apex deposition of General Star's parent, General Re, involved memoranda prepared by General Re executives that discussed revisions to its affiliates' policies for dealing with managing general agents. The memoranda were evidently prepared in response to the

[26] *Id.* at 821-22.
[27] *Id*. at 822 & n. 2.
[28] *Id*. at 822 & n. 5.
[29] *See, e.g.*, Evans, *supra* n. 7, at 519 (denying deposition of apex official, in part, on the grounds that plaintiffs could have received, and did receive, the information from less intrusive sources); *In re Burlington*, supra n. 21, at 327 (imposing burden on parties seeking to take an apex deposition to "make a good faith effort to obtain the discovery through less intrusive means).
[30] *See* Folwell, *supra* n. 5, at 175 (allowing deposition of Sara Lee President and CEO to go forward only after plaintiffs had taken Sara Lee's Fed. R. Civ. P. 30(b)(6) witness(es) and could show those deponents could not adequately provide discovery on certain enumerated subjects).
[31] *See* Digital Equip. Corp., *supra* n. 16, at 743 (holding that motive to bring a patent claim is not relevant).
[32] *See, e.g.*, Travelers Rental Co., Inc. v. Ford Motor Co., 116 F.R.D. 140, 146 (D. Mass. 1987) (allowing deposition of high-level corporate officers to determine motive and intent in instituting and administering the plan at issue; Rolscreen Co. v. Pella Prods. of St. Louis, Inc., 145 F.R.D. 92, 97 (S.D. Iowa 1992) *(*permitting deposition of president to examine corporation's motive for conditions set forth in conditional notice of termination); General Star Indem. Co. v. Platinum Indem., Ltd., 210 F.R.D. 80 (S.D.N.Y. 2002).
[33] General Star, *supra* n. 28, at 81.

"Unicover situation," which was an issue not widely known about within the company.[34] Thus, the court ordered the deposition of the executives who drafted the memoranda to discuss, among other subjects, the motivations and facts that led to their issuance.[35]

Even where the deposition is allowed for motive purposes, courts will impose reasonable limits on the scope of the deposition. For example, courts may require parties inquiring into corporate motives to depose lower-level employees first.[36] Courts may also limit the scope or the length of the deposition to guard against parties that may try to use the deposition to harass the executive.[37]

D. The Use of Extraordinary Writs To Bar Apex Depositions

It is possible that a trial court may order an apex deposition despite the policy underlying the Apex Doctrine. For example, courts may feel that the executive has more personal knowledge than he or she actually does, or that the plaintiff has exhausted less intrusive means of obtaining needing discovery. There is ample authority from multiple state court jurisdictions to support the use of writs of prohibition and mandamus to obtain immediate relief from an appellate court when a protective order seeking to stop or limit an apex deposition is wrongly denied.[38] Parties seeking relief by extraordinary writ, however, generally must demonstrate that the trial court abused its discretion or violated a legal duty *and* that the aggrieved party has "no adequate remedy by appeal."[39] However, so far, no cases appear to have been reported in the federal system where this relief has been sought.

E. Practice Advice About Apex Depositions

Usually, the cast of witnesses in every case is defined in the early stages of litigation. In those instances where an apex deposition may occur, the Apex Doctrine still offers the opportunity to seek limits or controls in an effort to minimize the disruption associated with the deposition. Counsel should be prepared to advocate for controls contingent on the court denying a protective order seeking to stop the deposition or denying the writ of mandamus.

Initial disclosures or responses to interrogatories seeking the identity of persons with discoverable information usually afford the first opportunity to define the potential witnesses in the case. The presence of an apex employee's identity in those disclosures can trigger the initial need to consider invoking the Apex Doctrine. The absence of an apex employee identified

---

[34] *Id.* at 82.

[35] *Id.* at 83-84.

[36] *Id.* at 83 (noting that the defendants first took the deposition of a lower level employee that General Re proffered, but that the lower level employee had no knowledge of the "Unicover situation"); Rolscreen, *supra* n. 28, at 98-99 (requiring plaintiffs to take the deposition of lower level employees whom the defendant claimed had more direct personal knowledge first); Liberty Mutual, *supra* n. 19, 10 Cal App. 4th at 1289 (requiring party seeking apex depositions to first obtain the needed discovery through less-intrusive means).

[37] Rolscreen, *supra* n. 28, at 98-99 (barring duplicative discovery in the president's deposition, and limiting it to 8 hours in one day).

[38] *In re* BP Prods. N. Am., Inc., No. 01-06-00613, 2006 Tex. App. LEXIS 6898 (Tex. App. — Houston Aug. 4, 2006, orig. proceeding) (granting a condition writ of mandamus directing the trial court to vacate its order striking a corporate executive's affidavit for allegedly being "insufficient" and reinstating the corporation's motion for protective order); Messina., *supra* n. 5, at 609 (granting a writ of prohibition to stop the deposition of Ford executives); Burlington, *supra* n. 21 (conditionally granting a writ of mandamus); Liberty Mutual, *supra* n. 19 (granting peremptory writ of mandate requiring the superior court to enter a protective order).

[39] *See, e.g.*, Walker v. Packer, 827 S.W.2d 833, 839 (Tex. 1990) (citations omitted); Messina, *supra* n. 5, at 607.

in early discovery disclosures may support an argument that a subsequent deposition notice for a previously unidentified apex employee is disingenuous and intended to harass.

The Rule 26(f) planning conference also is intended to flush out discovery issues and counsel should be prepared to explain the discovery needs and discovery defenses at play in the case. Before a protective order can be available in most jurisdictions, there usually is a meet and confer requirement – and the party seeking protection must explain the attempts made to resolve the discovery dispute without court intervention. *See* Fed. R. Civ. P. 26(c). With the assumption that the client wishes to evade the unauthorized oversight or inquiry of high ranking officers, efforts to resolve the discovery dispute should be documented in the Rule 26(f) written report, or in the Rule 16(b) planning conference report. Counsel should be prepared to identify alternate employees who may have adequate relevant knowledge, suggest Rule 29 stipulations to regulate the progression of other discovery before an Apex deposition can occur, remind opposing counsel of the availability of depositions on written questions under Rule 31 or interrogatories per Rule 33, and encourage Rule 30(b)(6) depositions of corporate designees "most knowledgible" on specific matters of needed discovery.

Where no cooperation is forthcoming, counsel should advise the court as early as possible that a Rule 26(c) motion might be forthcoming if the parties cannot resolve their differences. This said, Rule 26(c) offers the baseline of relief to be sought as an alternative to a deposition not going forward. Rule 26(c) sets forth some specifics limiting the breadth of an Apex Deposition:

> Upon motion by a party or by the person from whom discovery is sought . . . and for good cause shown, the court . . . may make any order which justice requires to protect a party or a person from annoyance, embarrassment, oppression or undue burden or expense, including one or more of the following . . .
>
> (1) that the disclosure or discovery not be had;
> (2) that the disclosure or discovery may be had only on specified terms or conditions including a designation of the time or place;
> (3) that the discovery may be had only by a method of discovery other than that selected by the party seeking discovery;
> (4) that certain matters not be inquired into, or that the scope of disclosure or discovery be limited to certain matters;
> (5) that discovery be conducted with no one present except persons designated by the court;
> (6) that a deposition after being sealed, be opened only by order of the court;
> (7) that a trade secret or other confidential research, development, or commercial information not be revealed or revealed only in a designated way. . . .

Each of these limitations is potentially applicable to any apex deposition. The video deposition of the CEO for a publicly traded company can be distributed almost instantly anywhere on the globe, and a "bad deposition" could damage investor relations or otherwise impact the level of litigation against the company, so counsel might seek an order that the deposition be transcribed in written format only, or that it be sealed or used only for purposes of the present litigation. A telephone deposition does not preclude the possibility of competitors or hostile press on the telephone call, so, counsel for the company should consider a safe and secure venue for the deposition with specified persons in attendance. For that matter, outsiders normally are not precluded from attending any deposition by any specific procedural rule, so, even where there is a traditional stenographic deposition

notice served, counsel should insure that only "insiders" to the litigation will be in attendance.[40]

If a subpoena is served for records production along with a *duces tecum* request seeking broad categories of documents, counsel should seek an order narrowing the categories of documents to be produced so as to eliminate a future attempt to re-open the deposition because of an asserted failure to search for or produce all documents at or before the deposition. The Federal discovery Rules presume that depositions can last seven hours, but, absent exceptional circumstances, if all other reasonable attempts have been made to discover evidence in alternate ways, the amount of time for the executive's deposition should only be a very small fraction of the presumed duration. Above all, if the party seeking the discovery has followed the Apex Doctrine guideline by seeking the information via other discovery means, the scope of the executive's deposition should be defined by the party seeking the discovery – so, an order from the court should limit the scope of the deposition to exactly that which is needed.

Additionally, in most significant litigation, the parties usually consider a confidentiality order for commercially sensitive information. Safeguards directed to discovery abuse generally, and on depositions specifically, should be incorporated into the confidentiality order. Typically, depositions can be designated "confidential", subject to the terms of the order, so that the deposition transcript is used only for purposes of the pending litigation and returned or destroyed at the close of the case. Provisions in a confidentiality order are supplemental, and can provide some level of protection after a deposition occurs, but should not be relied on as a substitute to seek controls on the deposition ahead of the deposition.

Finally, the apex deponent's statements probably will be deemed to be binding admissions under Fed. R. Evid. 801(d)(2),[41] and pursuant to Rule 32(a)(2), can be used in court proceedings for any purpose.[42]

Conclusion

An apex deposition is problematic at every level, and counsel for the corporation should not treat a notice for them lightly. While there may be growing favor within the judiciary to impose the limitations set forth in *Rule 26(c)* or similar state procedural rules, there may still be a philosophy that liberal discovery is favored. In those circumstances, counsel should strive to obtain controls on the deposition. Clearly, where counsel can demonstrate that the intent of the deposition is to harass or place the litigant in some disadvantage, by subjecting the litigant to unnecessary expense and inconvenience of lengthy depositions of its key executives, the Apex Doctrine should operate to at least limit, if not stop, the deposition. Even where a high ranking officer has some relevant knowledge, counsel should seek judicial intervention to require the opposing party to

[40] Some courts, such as the U.S. District Court for the District of Connecticut, provide specific procedures whereby parties may obtain orders making depositions private. *See* D. Conn. Loc. R. 30(a). More generally, because most depositions take place in private conference rooms, counsel's ownership or tenancy interest in the space can serve as a basis to exclude outsiders. DAVID M. MALONE, DEPOSITION RULES 4 (2D ED. 1998).

[41] *See, e.g.*, Ries Biologicals, Inc. v. Bank of Santa Fe, 780 F.2d 888, 890-91 (10th Cir. 1986) (holding that correspondence from bank senior vice president with substantial relevant authority within the bank did not constitute hearsay); Hybert v. Hearst Corp., 900 F.2d 1050, 1053 (7th Cir. 1990) (holding that statements made by a plant supervisor that workers in their 60s were likely to be laid off were admissible in age discrimination suit, as they were direct warnings made by management).

[42] *See, e.g.*, Pfotzer v. Aqua Systems, Inc., 162 F.2d 779, 785 (2d Cir. 1947); SEC v. American Realty Trust, 429 F. Supp. 1148, 1178 (E.D. Va. 1977).

exhaust all reasonable methods to discover the same information. Once there is a demonstration that any information to be derived from the targeted executive would be duplicative or cumulative, appropriate relief should be available.

Discovery of the Insurer's Claims File: Exploring the Limits of Plaintiff's Fishing License

By: Kathy J. Maus and John V. Garaffa [1]

I. Introduction

Every defense counsel has been confronted with discovery from Plaintiff's counsel that demands some variation of "A complete copy of the entire claims file, cover to cover, including both sides of any jacket, including all notes, memoranda, and diaries, pertaining to the claim that is the subject of this litigation up until the date that the instant suit was filed." Such a demand is objectionable as made, but understanding and articulating the basis for the objection will often mean the difference between successful opposition to the demand and an order to produce much if not all of the items requested.

It has long been true that merely noting that Plaintiff's request constitutes a "fishing expedition" is not a valid objection to discovery.[2] In general, the scope of modern discovery suggests that demands for production can be broad, even encompassing material that both sides recognize will not be admissible at a trial of the actual facts at issue. The motivation for requesting such material can be the search for facts that lead to admissible evidence, an entirely permissible goal. However, in today's litigation environment, discovery in individual cases is increasingly a vehicle for the collection of evidence to be studied, shared and used to build later cases against the defendant by large plaintiffs' firms or affiliated plaintiffs' counsel in other jurisdictions. Regardless whether true, the insurer's claims file is perceived as a potential gold mine of such information. As a consequence, defense counsel for insurers should be increasingly vigilant to protect their clients by taking steps to ensure that disclosures in individual cases are limited, as much as possible, to the proper discovery relevant to the facts actually at issue.

The purpose of this article is to outline the objections to Plaintiff's broad request for the insurer's claims file and the majority

Kathy J. Maus is the Managing Partner of the Tallahassee Office of Butler Pappas Weihmuller Katz Craig LLP, active in the firm's bad faith, casualty and first and third party liability defense and insurance coverage practices. Ms. Maus received her Bachelor of Science degree in Risk/Management & Insurance from Florida State University in 1986. She received her Doctor of Jurisprudence, with honors, from Florida State University in 1991. Ms. Maus is an IADC member.

John V. Garaffa is a Senior Associate in the Tampa office of Butler Pappas Weihmuller Katz Craig LLP, specializing in the defense of first party property insurance coverage matters. Mr. Garaffa received his Juris Doctor from the University of Minnesota, cum laude, in 1982 and his Master of Laws degree, with distinction, from Georgetown University in 1991.

---

[1] Butler Pappas Weihmuller Katz Craig, LLP jgaraffa@butlerpappas.com

[2] *See* J. A. Pike, The New Federal Deposition Discovery Procedure And The Rules of Evidence, 34 Ill. L. Rev. 1 (1939); A. Holtzoff, Instruments of Discovery Under Federal Rules of Civil Procedure, 41 Mich. L. Rev. 205 (1942); and Olson Transportation Co. v. Socony-Vacuum Oil Co., 8 Fed. R. Serv. 34.41, Case 2 (D.C. E.D. Wis. 1944), cited by, Hickman v. Taylor, 153 F.2d 212 (3d Cir. 1946). While the expansive view of the Third Circuit was limited by the U.S. Supreme Court in *Hickman v. Taylor*, 329 U.S. 495, 67 S.Ct. 385 (1947), the basic observation of the Third Circuit remains true.

rules governing successful objections by defense counsel to discovery of the materials in that file. Correctly applied, these rules permit defense counsel to resist an all encompassing demand like the one noted above, and respond appropriately to the more sophisticated attempts to achieve the same result by parsing the demand into discrete requests for the various components of the insurer's claims file.

II. Relevance: The General Rule of Discovery

The majority of U.S. jurisdictions have adopted the expansive view of discovery set out in Rule 26, Federal Rules of Civil Procedure. Subsection (b)(1) provides the general rule of thumb that anything is discoverable so long as it is relevant to the subject matter involved in the litigation. Rule 26 provides:

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

> (1) In General. Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(I), (ii), and (iii).

Under the majority rule, the basic restriction on plaintiff's request for the claims file, as in the case of a request for any material, is relevance. A review of the rules of civil procedure in the various states reveals this standard is broad and often subjective. The modern view is that material is relevant if it has any tendency to make the existence of any fact that is of consequence to the determination of the lawsuit more probable or less probable than it would be without the evidence.[3] The defect in Plaintiff's request for "the complete claims file" is that it simply fails to identify the material requested in a way that permits the Court to make a ruling on relevance and potential claims of privilege.

Simply put, there is a difference between "the claims file" as an object with all of it contents intact, and the documents contained within the file. For discovery purposes, the disparate types of documents within the insurer's claims file are no different than any similar collection of documents. In requesting that collection as an object, the Plaintiff makes the assumption that the mere presence of a document in that particular folder renders it relevant. The error of such an assumption was outlined by the Arizona Appellate Court in *Phoenix General Hospital v. Superior Court of Maricopa County.*[4]

In *Phoenix General Hospital* the plaintiff filed a motion to produce for inspection all books and records of the hospital corporation concerning financial operations of the hospital and its board of trustees since incorporation of the hospital. In rejecting the demand, the court held that the request was a blanket request not authorized by the rules of civil procedure permitting inspection and copying or photographing of designated documents. The court noted that it was committed to the liberal view of designation by categories where under the circumstances records are voluminous and hence it may be impossible

---

[3] Fed. R. Evid. 401.

[4] 402 P.2d 233 (Ariz. Ct. App. 1965).

to specifically designate each document sought. However, the essential factor in approving such a demand for discovery is that the category itself be sufficiently defined to aid the parties and so the court may understand with certainty the nature of the demand.[5] According to the court, the categories must be defined with sufficient particularity (i) to enable the opposing party to intelligently state any grounds for objection it may have to the requested production, and (ii) to enable the Court to intelligently rule on such objections.[6]

That certain materials within the typical claims file are subject to a basic relevancy objection is clear. In Florida, for example, the courts have determined that the insurer's claims file is not open to discovery simply because, as a matter of law, claim files, manuals, guidelines and documents concerning claim handling procedures of a homeowners' insurer are deemed irrelevant to a first-party dispute over the insurer's refusal to pay a claim under the policy.[7] While there is a temptation to view the Florida Court's ruling on requests for the claims file as a ruling on all its contents, an examination of subsequent cases shows that the focus is on whether the actual material within the file demanded falls within a privilege.

For example, in *Federal Ins. Co. v. Hall*,[8] Florida's Third District Court of Appeal granted certiorari and quashed the trial court's order to the extent that it ordered production of the adjustor's notes contained within the claims file. The court found that portion of the order constituted a departure from the essential requirements of law as the adjustor's notes were protected by the work-product privilege. In *State Farm Mut. Auto. Ins. Co. v. Cook*,[9] the insurer filed a motion to stay bad faith claims until the underlying issues of coverage were resolved. It also sought a protective order to avoid production of a number of documents relevant to the bad faith claims, including its claims files, litigation files, and internal operating manuals. The trial court denied both motions. In accordance with Florida law, the appellate court ruled that an insured's first-party action for benefits against the insurer had to be resolved before a cause of action for bad faith against the insurer accrued. Further, because the bad faith claims had to be stayed, the trial court's order denying a protective order for materials within the claims file was quashed insofar as it addressed materials relating to the bad faith claims.[10]

Similar rulings concerning the relevancy of claims file materials related to bad faith in litigation to determine coverage were reached by the Rhode Island Supreme Court in *Bartlett v. John Hancock Mut. L. Ins. Co.*,[11] and the Federal District Court of Montana in *In re Bergeson*.[12] A contrary ruling, permitting discovery, was entered by the Federal District Court for the Middle District of North Carolina in *Ring v. Commercial Union Ins. Co.*[13] However, the rationale for the court's decision in *Ring* is consistent with respect to the issue of relevancy as discussed in the earlier cases. In *Ring*, the Plaintiff's pleadings put bad faith at issue. As there would be one trial, the court denied the defendant's motion to bifurcate coverage and bad faith claims for discovery purposes, holding that it simply considered "it better to require that the discovery of the underlying contract claim

---

[5] *Id.* at 235.

[6] *Id.*

[7] State Farm Fire and Cas. Co. v. Valido, 662 So. 2d 1012 (Fla. Dist. Ct. App. 3d 1995).

[8] 708 So. 2d 976 (Fla. Dist. Ct. App. 3d 1998), citing American Reliance Ins. Co. v. Rosemont Condominium Homeowners Ass'n, Inc., 671 So. 2d 250 (Fla. Dist. Ct. App. 3d 1996), and State Farm Fire & Cas. Co. v. Valido, 662 So. 2d 1012 (Fla. Dist. Ct. App. 3d 1995).

[9] 744 So. 2d 567 (Fla. Dist. Ct. App. 2d 1999).

[10] *Id.*, citing State Farm Fire & Cas. Co. v. Martin, 673 So. 2d 518, 519 (Fla. Dist. Ct. App. 5th 1996); Michigan Millers Mut. Ins. Co. v. Bourke, 581 So. 2d 1368, 1370 (Fla. Dist. Ct. App. 2d 1991).

[11] 538 A.2d 997, 1000-01 (R.I. 1988).

[12] 112 F.R.D. 692, 697 (D. Mont. 1986).

[13] 159 F.R.D. 653, 658 (M.D.N.C. 1995).

and the bad faith claim proceed at the same time."[14]

(A) The Expected Contents of the Claims File

As it is the contents of the actual documents themselves that must be legally relevant to the issues before the court, it is helpful to consider what the plaintiff expects to find within the claims file. Those documents may be organized into five categories: (1) entries in a claims diary or log; (2) reports by outside investigators; (3) materials generated by the insurer's personnel and outside investigators such as statements taken from potential witnesses; (4) internal communications and memoranda, including case evaluations; and, (5) materials related to internal procedures and policies such as directives, guidelines and manuals. As noted above, all of these items may be relevant in a particular case and their presence within the "claims file" does not in itself insulate them from discovery. Rather, documents are discoverable unless they fall within the attorney-client or work product privileges.[15] While those privileges are discussed at length below, a brief review of some state court cases is instructive.

The North Carolina Appellate Court in *Evans v. United Services Auto. Assoc.*,[16] upheld the discovery of portions of the insurer's claims diary. In upholding the decision of the trial court, the *Evans* Court noted that, in the context of insurance litigation, determining whether a document was created in anticipation of that litigation is particularly challenging because the very nature of the insurer's business is to investigate claims; from the outset the *possibility* exists that litigation will result from the denial of a claim. Citing *Ring v. Commercial Union Ins.Co.*,[17] the court held that the general rule is that a reasonable possibility of litigation only arises after an insurance company has made a decision with respect to the claim of its insured.

Statements from witnesses contained within the insurer's the claims file have also been afforded protection under the work product privilege. However, the fact that the statements fell within the privilege did not ultimately prevent their discovery.[18] In *Fireman's Fund Ins. Co. v. McAlpine*,[19] the Rhode Island Supreme Court addressed the discovery of statements taken from eyewitnesses shortly after an event. The court noted that such statements taken immediately after an event "are unique catalysts in the search for truth in that they

---

[14] *Id.* at 656. Cf. Blake v. NW Ins. Co., 904 A.2d 1071, 1080 (Vt. 2006), and Howard v. Dravet, 813 N.E.2d 1217, 1221 (Ind. Ct. App. 2004) (no error when the trial court refused to order the production of the insurer's claims file as the sole remaining issue in the case was whether plaintiff was acting within the scope of his employment when the accident occurred, contents of the claims file were irrelevant to the actual issue before the court. The trial court abused its discretion by instituting a blanket privilege over the documents in the claim file; the privilege being invoked should be determined on a document-by-document basis).

[15] Some courts have referred to the Rule 26 protection afforded materials created in anticipation of litigation as a qualified privilege or qualified immunity. *See* Fireman's Fund Ins. Co. v. McAlpine, 120 R.I. 744, 391 A.2d 84 (1978); Evans v. United Services Auto. Assn, 142 N.C. App. 18, 541 S.E.2d 782 (N.C. App. 2001). *See also* 8 Charles Alan Wright et al., Federal Practice and Procedure § 2022, at 324 (2d ed. 1994).

[16] Evans, 142 N.C. App. 18, 541 S.E.2d 782 (N.C. Ct. App. 2001).

[17] 159 F.R.D. 653, 658 (M.D.N.C. 1995.)

[18] Johnston by Johnston v. Lynch, 574 A.2d 934, 937 (N.H. 1990), citing United States v. Murphy Cook & Co., 52 F.R.D. 363, 364 (E.D. Pa. 1971) (mere lapse of time is enough to justify production of material otherwise protected as work product).

[19] 120 R.I. 744, 775, 391 A.2d 84 (1978), citing McDougall v. Dunn, 468 F.2d 468 (4th Cir. 1972); Southern Railway Co. v. Lanham, 403 F.2d 119 (5th Cir. 1968); Teribery v. Norfolk & Western Railway, 68 F.R.D. 46 (W.D. Pa. 1975); Tiernan v. Westext Transport Inc., 46 F.R.D. 3 (D.R.I. 1969); Johnson v. Ford, 35 F.R.D. 347 (D. Colo. 1964); DeBruce v. Pennsylvania R. Co., 6 F.R.D. 403 (E.D. Pa.1947); Tinder v. McGowan, 15 Fed. R. Serv. 2d 1608 (W.D. Pa. 1970).

provide an immediate impression of the facts, the substantial equivalent of which cannot be recreated or duplicated by a deposition or interview months or years after the event." According to the court, the unique quality of such statements has been determined to provide special circumstances satisfying the undue hardship requirement needed to overcome their protection as work product. Nonetheless, the Court found that the plaintiff had failed to offer sufficient evidence to overcome the work product privilege of the insurer and quashed the trial court's order to produce the statements demanded by the plaintiff.[20]

(B) First Party Coverage Disputes

In the first party contract dispute between an insured and his or her insurer, such centers on the denial of all or part of the coverage for an insured's loss. Frequently the insured will attempt to focus the litigation on the behavior of investigators or adjusters and away from more objective evidence concerning the contract's provisions and the actual damage to the insured property. The Plaintiff hopes that by convincing the jury that the claim was handled poorly in the field or in a way which was inconsistent with the insurer's own internal guidelines, the jury will conclude the decision as to coverage was in error.

The first step in this process is usually a demand for the production of materials related to the insurer's internal manuals, guidelines and documents concerning claim handling procedures. As noted in *Valido*,[21] some state courts have rightly held that such demands are objectionable on relevancy grounds (as to the request for claims manuals, claims files, and operational guidelines). This position seems to be correct as, in the first party dispute, the actual facts at issue are the coverage provided by the policy, the nature of the damage claimed and the nature of the peril that the insured alleges resulted in the damage claimed. Whether the insurer's agents followed internal guidelines or procedures in the process of determining those facts is simply not relevant.

However, some states have taken the opposite view. In *Glenfed Development Corp. v. Superior Court*,[22] the case addressed whether the subcontractor's defective work was covered under the real estate developer's excess liability policy. The California Court of Appeal for the Second District, Division 1, found that the insurer's claims manual was discoverable in a first party dispute. In reaching its decision, the court admitted that there were no prior California cases specifically holding that an insurer's claims manual is discoverable. However, the court noted that California courts had recognized that claims manuals were admissible in coverage dispute litigation.[23] The court reasoned that if claims manuals are admissible, it follows that they are discoverable. It is important to note however that each of the cases cited by the *Glenfield* court involved claims for bad faith, where the insurer's adherence to it own procedures would arguably be relevant.[24]

---

[20] Cf. Recant v. Harwood, 222 A.D.2d 372 (N.Y. A.D. 1 Dept. 1995) (insured's statement to liability carrier protected from disclosure) and State Farm Fire and Cas. Co. v. Valido, 662 So. 2d 1012 (Fla. Dist. Ct. App. 3d 1995) (witness statements to liability carrier protected from disclosure).

[21] *Supra*.

[22] 53 Cal. App. 4th 1113 (Cal. Ct. App. 2 Dist. 1997).

[23] *Id.* at 1117, citing Neal v. Farmers Ins. Exchange, 582 P.2d 980 (Cal. 1978) (action seeking compensatory and punitive damages for "bad faith" failure to pay uninsured motorist benefits); Downey Savings & Loan Assn. v. Ohio Casualty Ins. Co. 189 Cal. App. 3d 1072 (Cal. App. 2 Dist. 1987) (bad faith action by the association against an insurance company for denial of benefits under a fidelity bond issued by the company); Moore v. American United Life Ins. Co., 150 Cal. App. 3d 610 (Cal. App. 3 Dist. 1984) (action for breach of a contract to provide disability benefits and bad faith denial of benefits).

[24] Cf. Blockbuster Entertainment Corp. v. McComb Video, Inc., 145 F.R.D. 402 (M.D. La. 1992)

The difficulty with the cases permitting discovery of claims file materials such as guidelines, manuals and internal documents relating to the insurer's opinions concerning contract construction, is that they appear to be inconsistent with the parole evidence rule. Generally, it is only when an insurance policy is ambiguous and susceptible of more than one reasonable interpretation, that extrinsic evidence may be admitted to resolve the ambiguity. If the court has not found the policy to be ambiguous, such evidence should not be relevant to the issues before the court. Under the circumstances, discovery of such evidence regarding the contract seems to violate the limits of discovery under the rules of civil procedure in most jurisdictions.

Certainly, if the language of an insurance policy is fairly susceptible to more than one different interpretation, the court can determine the parties' intent by examining extrinsic evidence.[25] In such a case, the plaintiff can present internal insurer documents such as the policy's drafting history, or manual provisions related to the policy, to assist in determining a reasonable construction. Once at issue, these materials are clearly relevant and thus discoverable. Similarly, where the policy is indefinite, equivocal, or ambiguous with respect to the subject matter, persons or interests insured, or the policy beneficiaries, such evidence is admissible, and thus relevant for the purposes of discovery, to resolve those questions.[26] However, the relevance of such materials arises after the court finds an insurance clause ambiguous. Materials such as the policy's drafting history cannot be used to find a clause ambiguous.[27]

A close examination of the cases and the reasoning employed by the courts indicates that, in a first party dispute where the issue is coverage, and there is no determination of ambiguity, discovery of the insurer's internal manuals, guidelines and documents concerning its claims handling procedures should be denied on the grounds of relevance. Discovery of other materials related to the claim such as investigative reports, photos, and internal memorandum will be subject to discovery provided the insured can satisfy the court that they are not protected by the work product privilege, or that the substantial equivalence of same cannot be otherwise obtained.

(plaintiffs had to prove that the policy provided coverage for the insured defendants' wrongful acts; therefore, any denial of coverage entitled the plaintiffs to explore the basis for denying coverage during discovery, including claim forms, manuals and other materials related to coverage, claims, claims processing, and claims similar to the ones in the case before the court) and Champion Intern. Corp. v. Liberty Mut. Ins. Co., 129 F.R.D. 63 (S.D.N.Y. 1989) (even recognizing extrinsic evidence of contract interpretation was irrelevant, the court ordered production of claims manuals discussing the disputed policy provisions for the period of coverage, "how-to-sell instructions" or guidelines for the period of coverage, drafting history documents, loss runs for the period starting from coverage on forward, and documents concerning the insurer's document retention or destruction policy). *See also*, Hoechst Celanese Corp. v. National Union Fire Ins. Co. of Pittsburgh, 623 A.2d 1099 (Del. Super. Ct. 1991) (where policy language was ambiguous, information relating to interpretation and drafting history of the policy language, and information concerning the association between insurers, trade organizations and committees who drafted the policies of insurance, were discoverable).

[25] 44A Am. Jur. 2d Insurance § 2016 citing Cle Elum Bowl, Inc. v. North Pacific Ins. Co., Inc., 96 Wash. App. 698, 981 P.2d 872 (Div. 3 1999). As to the use of extrinsic evidence to construe ambiguous instrument, S*ee generally* :29A Am. Jur. 2d, Evidence § 1134.

[26] 44A Am. Jur. 2d Insurance § 2016, citing Howard Fire Ins. Co. v. Chase, 72 U.S. 509, 18 L. Ed. 524 (1866); Drisdom v. Guarantee Trust Life Ins. Co., 371 So. 2d 690 (Fla. Dist. Ct. App. 3d Dist. 1979).

[27] 44A Am. Jur. 2d Insurance § 2016, citing Cook v. Evanson, 83 Wash. App. 149, 920 P.2d 1223 (Div. 1 1996).

(C) First and Third Party Bad Faith Disputes

As touched on in the discussion above, first and third party "bad faith" claims present different issues and thus different outcomes in disputes over demands for discovery of an insurer's claim and litigation files. That said, the guiding principle again appears to be the relevance of the requested material to the facts at issue before the court. While a detailed treatment of bad faith is beyond the scope of this article, some basics are important to underscore the nature of the evidence that will be relevant in such suits.

The basis for the tort of bad faith is the "implied covenant of good faith and fair dealing," which is imputed into insurance policies. Often the inquiry will center on whether an insurance company's conduct was inconsistent with "the very protection or security which the insured sought to gain by buying insurance."[28] While the cause of action is subject to different common law and statutory elements in each state,[29] bad faith may generally be found where the insurance company acts in a way that unreasonably deprives the policyholder of the benefits due under the policy.[30]

Insurance bad faith actions involve either first party or third party coverage. Generally, in a first party situation, the implied duty of good faith and fair dealing is breached if the insurance company (1) acts unreasonably in delaying or denying policy benefits and (2) acts knowingly or with reckless disregard as to the unreasonableness of its delay or denial.[31] In the third-party context, the implied duty of good faith and fair dealing is alleged to be breached if the insurance company, exercising exclusive authority to accept or reject settlement offers, and with the exclusive right and obligation of defending the claim, does so in a manner that results in an judgment against its insured that is in excess of the policy limits.[32]

While necessarily abbreviated, the description of both first and third party bad faith highlights the factual difference between an insured's suit on the issue of coverage and a suit for first or third party bad faith. As noted above, in the coverage dispute, the actual facts at issue are those which will determine coverage provided by the policy. The precise manner in which the insurer reached its decision and its internal documents, such as guidelines, manuals, and documents detailing the insurer's motivations, are not relevant as they will not tend to make the facts at issue more or less likely.

In the first and third party bad faith case, however, the focus of the litigation will be on the insurer's handling of the claim, its motivations and the adherence of the insurer and its agents to internal manuals and guidelines. As those facts are at issue in the bad faith case, evidence tending to show how the insurer adjusted the claim and why it did what it did are relevant, and the materials related to those

---

[28] *Id.* Citing Rawlings v. Apodaca, 726 P.2d 565, 571 (Ariz. 1986), Kan. Bankers Sur. Co. v. Lynass, 920 F.2d 546, 548 (8th Cir. 1990); State Farm Mut. Auto. Ins. Co. v. Weiford, 831 P.2d 1264, 1266 (Alaska 1992); Walter v. Simmons, 818 P.2d 214, 223 (Ariz. Ct. App. 1991); Pemberton v. Farmers Ins. Exch., 858 P.2d 380, 382 (Nev. 1993); Pavia v. State Farm Mut. Auto. Ins. Co., 626 N.E.2d 24, 27 (N.Y. 1993); Austin Co. v. Royal Ins. Co., 842 S.W.2d 608, 610 (Tenn. Ct. App. 1992) and Koehrer v. Super. Ct., 226 Cal. Rptr. 820, 828 (Ct. App. 1986).

[29] Nelson v. State Farm Mut. Auto. Ins. Co., 988 F. Supp. 527, 533 fn 10 (E.D. Pa. 1997) ("It is nearly impossible to state with certainty the exact number of states recognizing a cause of action for bad faith or to classify the exact standards that they have established.").

[30] Randy Papetti, The Insurer's Duty of Good Faith in the Context of Litigation, 60 Geo. Wash. L. Rev. 1931 (1992).

31 Chris Michael Kallianos, Survey, Bad Faith Refusal to Pay First-Party Insurance Claims: A Growing Recognition of Extra-Contract Damages, 64 N.C. L. Rev. 1421, 1435 (1986).

[32] Robert E. Keeton, Liability Insurance and Responsibility for Settlement, 67 HVLR 1136 (1954).

facts will be subject to discovery. However, discovery of those documents is not unfettered as many of the documents sought are still subject to assertions of work product and/or attorney-client privilege, trade secret, confidentiality or other protections. As the court stated in *Dixie Mill Supply Co., Inc. v. Continental Cas. Co.*, "[W]hile arguably it may be more difficult to prove a claim of bad faith failure to settle without examining an insurance company's claims file, that does not mean it is impossible."[33] Highlighting that an allegation of bad faith is not a license to embark upon a fishing expedition, the court held "[A] simple assertion that an insured cannot otherwise prove her case of bad faith does not automatically permit an insured 'to rummage through [the insurers'] claims file.'"[34]

However, the court in *Reavis v. Metropolitan Property and Liability Ins. Co.*[35] was far more accommodating to plaintiff's assertion that access to at least a portion of the insurer's claims file was critical to her case. The court held that the claims file is a unique, contemporaneously prepared history of the company's handling of the claim and that, in a bad faith action such as the plaintiff's, the need for the information in the file was not only substantial but overwhelming. The court further held that the "substantial equivalent" of the requested material could not be obtained through other means of discovery.[36]

While expansive in its treatment of work product, the court made its decision under the rubric of the "substantial need doctrine" contained in Rule 26, not on the basis that a claim for bad faith waived the work product privilege. The court declined to order production of correspondence between defendant and its attorney or correspondence between the insurer and its insureds finding that it was protected by the attorney-client and work product privilege. On those grounds, the court also found that the recorded statements given by the insureds to the insurer's claims representative were privileged.[37]

The insurer's position with respect to demands for materials in the claims file is perhaps best stated by the court in *Ferrara & DiMercurio, Inc. v. St. Paul Mercury Ins. Co*.,[38] where the court rejected the claim that the mere assertion of a bad faith claim operates to change the rules governing the production of material protected by the attorney-client or work product privilege. The court held "Rule 26(b)(3), . . . does not expressly create an exception for work product material generated in a first party bad faith insurance action. Barring such language, it is inappropriate to treat first party bad faith insurance actions differently vis-a-vis other types of actions."[39] In responding to plaintiff's discovery requests, it will be the nuances of the attorney-client and work product privileges, discussed at length below, that will govern the success of a defendant's efforts to keep discovery to its proper limits.

III. Attorney-Client Privilege

Once the court has determined that the materials requested from the insurer's claims file are relevant to the facts at issue in the litigation, it will be for the insurer to assert that the documents requested are nonetheless protected from discovery. The two primary grounds for such protection are the attorney-client privilege and the derivative and more recent attorney work product doctrine.

While closely related, the two types of protections are, in theory, intended to shield different materials from discovery. However, as the cases illustrate, the precise

[33] 168 F.R.D. 554, 559 (E.D. La. 1996), citing Ring v. Commercial Union Ins. Co., 159 F.R.D. 653, 658 (M.D. N.C. 1995).

[34] *Id.*

[35] 117 F.R.D. 160 (S.D. Cal. 1987).

[36] *Id.* at 164 (internal citations omitted).

[37] *Id.*

[38] 173 F.R.D. 7 (D. Mass. 1997).

[39] *Id.* at 11.

line between attorney-client material and attorney work product is somewhat imprecise, and differs from jurisdiction to jurisdiction. The consequence of these differences may mean that, depending on the facts in an individual case, material protected in one jurisdiction may be discoverable in another. While an exhaustive review of the rules in the various states is beyond the scope of this article, the discussion below will highlight the primary factors upon which a court's decision to extend protection or permit discovery will turn.

(A) The Origin and Purposes of the Attorney-Client Privilege

The attorney-client privilege is one of the oldest recognized privileges for confidential communications.[40] The privilege is said by some to have had its origins in Roman law. The privilege is intended to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice."[41] As Lord Chancellor Brougham observed in 1833 in *In Greenough v. Gaskell*:[42]

> The foundation of this rule is not difficult to discover. It is not (as has sometimes been said) on account of any particular importance which the law attributes to the business of legal professors, or any particular disposition to afford them protection . . . But it is out of regard to the interests of justice, which cannot be upholden, and to the administration of justice, which cannot go on without the aid of men skilled in jurisprudence, in the practice of the courts, and in those matters affecting rights and obligations which form the subject of all judicial proceedings. If the privilege did not exist at all, everyone would be thrown upon his own legal resources. Deprived of all professional assistance, a man would not venture to consult any skillful person, or would only dare to tell his counselor half his case.

Recognized at common law,[43] federal[44] and state law,[45] the attorney-client privilege protects confidential communications made between clients and their attorneys when the communications are for the purpose of securing legal advice or services.[46]

(B) The Elements of the Privilege

In *U.S. v. United Shoe Machinery Corp.*,[47] Judge Wyzanski advised that the attorney-client privilege applies only if:

(1) the asserted holder of the privilege is or sought to become a client;
(2) the person to whom the communication was made
    (a) is a member of the bar of a court, or his subordinate and
    (b) in connection with this communication is acting as a lawyer;
(3) the communication relates to a fact of which the attorney was informed
    (a) by his client
    (b) without the presence of strangers
    (c) for the purpose of securing primarily either
        (i) an opinion on law or
        (ii) legal services or

---

[40] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981), citing 8 John H. Wigmore, Evidence, § 2290 (McNaughton rev. 1961); Hunt v. Blackburn, 128 U.S. 464, 470 (1888).

[41] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

[42] 1 Myl. & K. 98, 103 (1883), cited by *In re* Selser, 105 A.2d 395, 401 (N.J. 1954).

[43] U.S. v. Zolin, 491 U.S. 554 (1989).

[44] *See* Fed. R. Evid. 501.

[45] *See, e.g.*, West's Tennessee Code Annotated § 23-3-105.

[46] *In re* Lindsey, 148 F.3d 1100, 1103 (D.C. Cir. 1998).

[47] 89 F.Supp. 357, 358 (D.C. Mass. 1950).

(iii) assistance in some legal proceeding, and not
(iv) for the purpose of committing a crime or tort; and

(4) the privilege has been
(a) claimed and
(b) not waived by the client.

While the rule varies somewhat in different jurisdictions, Judge Wyzanski's opinion has been widely accepted as correctly setting out the parameters of the attorney-client privilege[48] The North Carolina court in *Evans v. United Services Auto. Ass'n*[49] stated the elements more succinctly, holding that a party may assert the attorney-client privilege if (1) the relation of attorney and client existed at the time the communication was made, (2) the communication was made in confidence, (3) the communication relates to a matter about which the attorney is being professionally consulted, (4) the communication was made in the course of giving or seeking legal advice for a proper purpose, although litigation need not be contemplated, and (5) the client has not waived the privilege. Though more abbreviated, this statement of the privilege makes it clear that, notwithstanding the relationship between the attorney and the client, the client must have intended the communication to be confidential.[50]

(C) The Scope of the Privilege

When the privilege applies, it affords confidential communications between lawyer and client complete protection from disclosure.[51] However, as the privilege has the effect of withholding relevant information from the fact-finder, the courts have made it clear that the privilege applies only where necessary to achieve its purpose.[52] As stated by the U.S. Supreme Court in *Fisher v. U.S.*,[53] the privilege "protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege." Thus, while the privilege applies to confidential communications from the client to the lawyer, it may not protect communications from the lawyer to the client unless the facts show that the disclosure of the lawyer-to-client communications would directly or indirectly reveal the substance of the client's confidential communications to the lawyer.[54]

In the context of plaintiffs' efforts to discover the insurer's claims file, litigation has explored the limits of the privilege as it relates to the insured's communications with his or her insurer,[55] with the attorney hired by the insurer to defend the insured, and the attorney and the insurer. The cases that follow illustrate the limits of the privilege. Taken together, they show that

---

[48] *See* Hopewell v. Adebimpe, 18 Pa. D. & C.3d 659, 661 (1981); Perfection Corp. v. Travelers Cas. & Sur., 790 N.E.2d 817 (Ohio App. 8 Dist. 2003); Clausen v. National Grange Mut. Ins. Co., 730 A.2d 133 (Del. Super. 1997); Austin v. State, 934 S.W.2d 672 (Tex. Ct. App. 1996); State ex rel. U.S. Fidelity and Guar. Co. v. Montana Second Judicial Dist., 783 P.2d 911 (Mont. 1989); State ex rel. U.S. Fidelity and Guar. Co. v. Canady, 460 S.E.2d 677 (W. Va. 1995); People v. Belge, 59 A.D.2d 307 (N.Y. A.D. 1977); Hughes v. Meade, 453 S.W.2d 538 (Ky. 1970).

[49] 541 S.E.2d 782 (N.C. App. 2001).

[50] *See also*, State ex rel. Medical Assurance of West Virginia, Inc. v. Recht, 583 S.E.2d 80 (W. Va. 2003).

[51] Connecticut Indem. Co. v. Carrier Haulers, Inc., 197 F.R.D. 564 (W.D. N.C. 2000), citing Trammel v. United States, 445 U.S. 40, 50 (1980); In re Grand Jury Subpoena, 204 F.3d 516, 519-20 (4th Cir. 2000); Hawkins v. Stables, 148 F.3d 379, 383 (4th Cir. 1998).

[52] 425 U.S. 391 (1976).

[53] *Id.* at 403.

[54] Journal/Sentinel, Inc. v. School Bd. of School Dist. of Shorewood, 521 N.W.2d 165 (Wis. App. 1994), citing Jack Weinstein & Margaret Berger, Weinstein's Evidence, ¶ 503(b)[03] n. 5 at 503-56 to 503-57 (1991).

[55] For a detailed treatment of this aspect of the privilege, see John P. Ludington, Insured-Insurer Communications as Privileged, 55 A.L.R. 4th 336 (Originally published in 1987).

courts struggle with the tension between a preference for open discovery of relevant evidence and the derogation of the attorney-client privilege. In these cases, the courts examine the facts in light of the discrete elements of the privilege to see if discovery can be granted despite the arguable applicability of the privilege.

Highlighting the importance of the confidentiality element of the privilege, the court in *Dobias v. White*,[56] held the mere fact that the evidence relates to communications between attorney and client alone does not require its exclusion. According to the court, "only confidential communications are protected. If it appears by extraneous evidence, or from the nature of a transaction or communication that they were not regarded as confidential, or that they were made for the purpose of being conveyed by the attorney to others, they are stripped of the idea of a confidential disclosure and are not privileged."[570]

Similarly, even "confidential" communications between counsel and the insurer may not be privileged if the attorney was not acting as a legal advisor when the communication was made.[58] Thus, while the protection given to communications between attorney and client apply equally to in-house counsel,[59] an insurance company and its counsel may not avail themselves of the protection afforded by the attorney-client privilege if the attorney's advice relates to actions said to be in the company's normal course of business.

Consistent with this principle, the New York court, in *Bertalo's Restaurant Inc. v. Exchange Ins. Co.*,[60] held that reports made to the insurer by attorneys, employed to examine property damage claims before a decision had been made on coverage, were not protected from disclosure. The court noted that its review of the documents established that they consisted primarily of reports made by the attorneys who conducted the investigation of the claim on behalf of the defendant carrier, and communications from the carrier to those attorneys. The court held that the payment or rejection of claims is a part of the regular business of an insurance company. Consequently, reports which aid it in the process of deciding which actions to pursue are made in the regular course of its business.[61] Merely because such an investigation was undertaken by an attorney will not cloak the reports and communications with privilege.[62]

While it is clear that all communications with an attorney are not protected by the attorney-client privilege, courts have found that communications made by insureds to non-lawyer representatives of the insurer may nonetheless be protected from disclosure by the attorney-client privilege. The rational for this extension of the privilege is that, in some situations, such communications are made for the dominant purpose of transmission to an attorney assigned to defend the claim. Thus, the court in *State v. Pavin*,[63] held the privilege shielded communications between the insured and the insurer's adjuster where the communications were in fact made to the adjuster for the dominant purpose of the insured's defense by the attorney and where confidentiality was the insured's reasonable expectation.

---

[56] 83 S.E.2d 785, 788 (N.C. 1954).

[57] *Id.*

[58] Evans, *supra*. at 791.

[59] *See generally* Upjohn, *supra;* Shelton v. American Motors Corp., 805 F.2d 1323 fn. 3 (8th Cir. 1986).

[60] 240 A.D.2d 452, (N.Y.A.D. 2 Dept. 1997).

[61] *Id.*, citing Landmark Ins. Co. v. Beau Rivage Rest., 121 A.D.2d 98 (N.Y.A.D. 2 Dept. 1986).

[62] *Id.*, citing Spectrum Sys. Intl. Corp. v. Chemical Bank, 581 N.E.2d 1055 (N.Y. 1991).

[63] 494 A.2d 834 (N.J. 1985). *See also*, Jacobi v Podevels, 127 N.W.2d 73 (WI 1964); Langdon v. Champion, 752 P.2d 999 (AK 1988); DiCenzo v. Izawa, 723 P.2d 171 (Haw. 1986); Chicago Trust Co. v. Cook County Hosp., 698 N.E.2d 641 (Ill. Ct. App. 1 Dist.1998); Soltani-Rastegar v. Superior Court, 256 Cal. Rptr. 255 (Cal. Ct. App. 1 Dist. 1989).

Other courts have taken a more restricted view of such communications between the insured and the insurer. In *In Varuzza by Zarrillo v. Bulk Materials, Inc.*,[64] the court held that a written statement given by a motorist to an investigator for his insurer one week after the accident was not protected by the attorney-client privilege and was thus subject to discovery by a second driver in the accident underlying the motorist's action. The court found that the insurer asserting the privilege had failed to establish that an attorney-client relationship was even contemplated at the time of the statement. Instead, the court found that the statement was solicited by the insurer's investigator in accordance with the insurer's normal practice and not at the behest of or on behalf of an attorney.

(D) Waiver

Whether one adopts Judge Wigmore's elements or the North Carolina court's more abbreviated characterization of the privilege, it is clear that the attorney-client privilege may be waived. Such waiver may be express or implied.[65] An express waiver occurs when a client voluntarily discloses the content of privileged communications.[66] Generally, any such waiver is limited to the attorney-client communications on the matter disclosed or at issue.[67] An implied waiver occurs where the client has placed in issue a communication which goes to the heart of the claim in controversy.[68]

(1) The "At Issue" Doctrine

The "At Issue" doctrine is an exception to the attorney-client privilege and the work product doctrine and will result in the production of otherwise protected material. Courts applying the "at issue" doctrine in the context of insurance disputes have held that, where the facts contained in the otherwise privileged material have been placed in issue, a client may not invoke the attorney-client privilege as a shield for discovery.[69]

A party waives its privileges when (1) by some affirmative act, (2) the party makes the protected information relevant to the case, and (3) the opposing party is thereby denied access to information vital to its defense.[70] A number of courts have acknowledged the importance of the attorney-client privilege and the work product immunity and conclude that privileged information is "vital" only when the proponent of the privilege directly places the attorney's advice at issue in the litigation.[71]

It is important to note that the test enunciated above is a three part test. Thus, it is the affirmative act on the part of the party holding the privilege that must first be proved. Mere relevance of the attorney-client material is not the standard for determining whether or not evidence should be protected from disclosure as privileged. That remains the case even if one might conclude the facts to be disclosed are vital, highly probative, directly relevant or even go to the heart of the case.[72]

---

[64] 169 F.R.D. 254 (N.D. N.Y. 1996).

[65] 81 Am. Jur. 2d Witnesses § 348, at 322-23 (1992).

[66] Miller v. Continental Ins. Co., 392 N.W.2d 500, 504-05 (Iowa 1986) (privilege waived by the voluntary disclosure of the content of a privileged communication to a third party).

[67] *Id.* at 504-05.

[68] 81 Am. Jur. 2d Witnesses § 348, at 323 (1992).

[69] Hoechst Celanese Corp. v. National Union Fire Ins. Co. of Pittsburgh, 623 A.2d 1118, 1125 (Del. Super. 1992).

[70] Sax v. Sax, 136 F.R.D. 541, 542 (D. Mass. 1991); Hearn v. Rhay, 68 F.R.D. 574, 581 (E.D. Wash. 1975).

[71] *See, e.g.*, North River Ins. Co. v. Philadelphia Reinsurance, 797 F.Supp. 363, 370 (D.N.J. 1992); State v. Hydrite Chem. Co., 582 N.W.2d 411, 418-19 (Wis. Ct. App. 1998); Aranson v. Schroeder, 671 A.2d 1023, 1030 (N.H. 1995).

[72] Rhone-Poulenc Rorer Inc. v. Home Indem. Co., 32 F.3d 851 (C.A. 3 Pa. 1994). *See also* Arthur R. Miller & Richard L. Marcus, Federal Practice and Procedure at 253-54 (2d ed. 1994); Richard L.

Express reliance on an advice-of-counsel defense would constitute an implied waiver of the attorney-client privilege as to that advice.[73] The more difficult question is whether and when an assertion short of an express advice-of-counsel defense waives the privilege. In his treatise on evidence, Judge Wigmore stated, "[A] waiver is to be predicated not only when the conduct indicates a plain intention to abandon the privilege, but also when the conduct (though not evincing that intention) places the claimant in such a position, with reference to the evidence, that it would be unfair and inconsistent to permit the retention of the privilege. It is not to be both a sword and a shield. . ."[74] The mere denial of allegations in the complaint, or an assertion that the denial of benefits was in good faith, is not an implied waiver.[75] However, where the insurer advances its own interpretation of the law as a defense, including what its employees knew of the law, the insurer places the legal advice it was given at issue.[76]

In *State Farm Mut. Auto. Ins. Co. v. Lee*,[77] the Arizona Supreme court found the insurer had waived the attorney-client privilege despite its insistence that in was not asserting an "advice of counsel" defense. The court held:

> [A] litigant's affirmative disavowal of express reliance on the privileged communication is not enough to prevent a finding of waiver. When a litigant seeks to establish its mental state by asserting that it acted after investigating the law and reaching a well-founded belief that the law permitted the action it took, then the extent of its investigation and the basis for its subjective evaluation are called into question. Thus, the advice received from counsel as part of its investigation and evaluation is not only relevant but, on an issue such as this, inextricably intertwined with the court's truth-seeking functions. A litigant cannot assert a defense based on the contention that it acted reasonably because of what it did to educate itself about the law, when its investigation of and knowledge about the law included information it obtained from its lawyer, and then use the privilege to preclude the other party from ascertaining what it actually learned and knew."[78]

A contrary result was reached in *Dixie Mill Supply Co., Inc. v. Continental Cas. Co.*,[79] in which the plaintiff asserted that the insurer affirmatively placed at issue the advice of counsel defense by asserting that it acted in good faith in compliance with the insurance policies and their legal obligations. In rejecting that claim, the court held that, under Louisiana law, a party waives the attorney-client privilege only when he "pleads a claim or defense in such a way that he will be forced inevitably to draw upon a privileged communication at trial in order to prevail."[80]

(2) The "Common Interest" Doctrine

Generally, when an attorney acts for two different parties who each have a

---

Marcus, The Perils of Privilege: Waiver and the Litigator, 84 Mich. L. Rev. 1605, 1630 (1986).

[73] State Farm Mut. Auto. Ins. Co. v. Lee, 13 P.3d 1169 (Ariz. 2000). *See also* McCormick on Evidence § 93, at 373 (5th ed. 1999); 8 Charles A. Wright, Arthur R. Miller & Richard L. Marcus, Federal Practice and Procedure § 2016.2, at 253 (2d ed. 1994); McNeely v. Board of River Port Pilot Comm'rs, 534 So. 2d 1255, 1255-56 (La. 1988).

[74] 8 John H. Wigmore, *supra.* at § 2388, at 855, cited by Throop v. F. E. Young & Co., 382 P.2d 560 (Ariz. 1963).

[75] Lee, *supra*.

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] Dixie Mill Supply Co., Inc. *supra* at 556, citing Ring v. Commercial Union Ins. Co., 159 F.R.D. 653, 658 (M.D.N.C. 1995).

[80] *Id.*, citing Succession of Smith v. Kavanaugh, Pierson & Talley, 513 So. 2d 1138, 1145 (La. 1987).

common interest, communications by either party to the attorney are not necessarily privileged *in a subsequent controversy between the parties*. Under this doctrine, "when an attorney has been retained to represent both insured and insurer in a third party action, communications by either party will not be privileged . . . if their interests later diverge."[81]

The doctrine typically arises in the context of demands for attorney-client material in "bad faith" actions prosecuted by an insured against his insurer for failure to settle within the policy limits of a liability policy. The general rule is that communications between the insurer and an attorney, who also represented the insured in the original tort action against the insured, are not privileged with respect to the insured.[82] The justification for the denial of the claim of privilege is that the attorney retained to defend the underlying tort claim is representing the interests of both the insurer and the insured.

The decision of the Pennsylvania court in *O'Brien v. Tuttle*[83] provides some sense of the nuances of the doctrine. In *O'Brien*, the plaintiff filed a complaint for medical malpractice. Shortly after forwarding the complaint in the lawsuit to his insurance carrier, the insurer sent the defendant doctor a questionnaire regarding the claim. The doctor completed the questionnaire and gave it to the attorney furnished by his insurance carrier to defend the lawsuit rather than returning the completed questionnaire to his insurance carrier, and thereafter asserted attorney-client privilege in response to a request for its production. The attorney later forwarded a copy of this questionnaire to the insurance carrier.

The court observed that if counsel was acting as counsel for both the doctor and his insurance carrier, the communication would be protected. The court found that the law recognizes a joint representation by a common attorney for the mutual benefit of two or more parties and thus, in this situation, the law extends the attorney-client privilege to any communication among the parties and their counsel in order to permit the free flow of information.[84]

On the waiver issue, the court noted there was a question about whether the privilege would be waived if the client had not authorized the transmission of the form by the attorney to the carrier because it is the client who is the holder of the privilege and only a client or his or her attorney, acting with the client's authority, may waive the privilege.[85] In addition, if the disclosure was made to further the insured's interests in connection with counsel's preparation of the litigation (e.g. to encourage the insurance carrier to settle its claim), it can be argued that the disclosure does not constitute a waiver of the attorney-client privilege.[86]

The case of *Dedham-Westwood Water Dist. v. National Union Fire Ins. Co. of Pittsburgh* is an example of the outer edges of the common interest doctrine.[87] While facts of the underlying litigation are complex, the discovery arose in an action by the plaintiff against insurers, following settlement of an environmental claim.

---

[81] Hoechst Celanese Corp. v. National Union Fire Ins. Co. of Pittsburgh, Pa., 1995 WL 411805 (Del. Super. Ct. 1995).

[82] *See* Baker v. CNA Ins. Co., 123 F.R.D. 322 (D. Mont.1988), citing Gibson v. Western Fire Ins. Co., 682 P.2d 725 (Mont. 1984); Longo v. American Policyholders Ins. Co., 436 A.2d 577 (N.J. 1981); Simpson v. Motorists Mutual Ins. Co., 494 F.2d 850 (7th Cir. 1974) (applying Ohio law), cert. denied, 419 U.S. 901 (1974); Dumas v. State Farm Mutual Auto Ins. Co., 274 A.2d 781 (N.H. 1971); Shapiro v. Allstate Ins. Co., 44 F.R.D. 429 (D.C. Penn. 1968); Chitty v. State Farm Mutual Automobile Ins. Co., 36 F.R.D. 37 (D.C.S.C. 1964).

[83] 21 Pa. D. & C. 3d 319 (Pa. Com. Pl. 1981).

[84] *Id.* at 321.

[85] *Id.* at fn 2, citing McCormick on Evidence, §97.

[86] *Id.* citing State v. Pratt, 398 A.2d 421 (Md. 1979); State v. Mingo, 392 A. 2d 590 (N.J. 1978); Pouncy v. State, 353 So. 2d 640 (Fla. Dist. Ct. App. 1977). Cf.

[87] Dedham-Westwood Water Dist. v. National Union Fire Ins. Co. of Pittsburgh, 2000 WL 33593142 (Mass. Super. 2000).

The court's final comment in *Dedham-Westwood, supra,* suggests potential grounds for narrowing the doctrine even in those cases where the insurer participates in the underlying action. The court observed that the "common interest" doctrine is less appropriate when the documents at issue were prepared in an atmosphere of uncertainty as to the scope of identity of interest shared by insurer and insured.[88] As the court noted, "Particularly in the environmental liability context, the insured often enters and acts in the underlying litigation alone, with an apprehension of not only the outcome of that litigation, but also of the foreboding litigation with its insurers."[89] Under these circumstances, the argument that there was no reasonable expectation of privacy due to an identity of interest is "fiction," and the "common interest" exception cannot apply.

(3) The Crime Fraud Exception

Item C.(3)(d) of Judge Wyzanski's statement of the attorney-client privilege in *U.S. v. United Shoe Machinery Corp*, *supra*, provides that the privilege does not apply if the communication was for the purpose of committing a crime or tort. This exception to the privilege has been invoked for a wide variety of offenses including fraudulent pleadings, fraudulent insurance claims and conspiracy to fraudulently obtain a default judgment.[90]

The precise conduct that may give rise to the crime fraud exception has been disputed. The Court, in *In re Sealed Case*,[91] held that work-product materials may be subject to discovery if "the client actually committed or attempted a crime or fraud subsequent to receiving the benefit of counsel's work product."[92] Taking a more limited view, the court, in *The Pritchard-Keang Nam Corp. v. Jaworski*,[93] held that it is not enough that the alleged fraud merely follow the attorney-client communication. Instead, for the crime-fraud exception to apply, the legal advice must be sought or obtained in furtherance of or in relation to the fraudulent activity.[94]

There is also the suggestion that the standard for invoking the crime fraud exception with respect to work product may be different from that applied in the context of material protected by the attorney-client privilege. The court, in *In re Murphy*,[95] found that, as Rule 26(b)(3) protects a broader and, to some extent, different type of material than the attorney-client privilege, the traditional exceptions to the attorney-client privilege cannot be automatically engrafted onto the work product doctrine. According to the court, a careful analysis must be undertaken to ascertain whether or not the adoption of such an exception would be consistent with the purpose and proper functioning of the work product privilege.[96]

The court in *In re Murphy* formulated the following test for the use of the crime fraud exception in cases where the material demanded was otherwise protected as work product:

> If there is a crime or fraud exception to the work product privilege that would justify discovery of opinion work product, the party seeking discovery has

---

[88] *Id.* at 5, citing Remington Arms Co. v. Liberty Mut. Ins. Co., 142 F.R.D. 408 (D.Del.1992).

[89] *Id.*, citing Pittston Co. v. Allianz Ins. Co., 143 F.R.D. 66, 70-71 (D.N.J.1992.)

[90] *See, e.g.*, United Services Auto. Assoc. v. Werley, 526 P.2d 28 (Alaska 1974) and the cases cited therein.

[91] 676 F.2d 793 (D.C.Cir.1982)

[92] *Id.* at 815, citing *In re* Grand Jury Proceedings, 604 F.2d 798 (C.A. Pa. 1979) and *In re* Murphy, 560 F.2d 326 (C.A. Minn. 1977).

[93] 751 F.2d 277 (C.A. Mo. 1984).

[94] *Id.*, citing *In re* Grand Jury Subpoena Duces Tecum, 731 F.2d 1032, 1039 (2d Cir. 1984) (crime or fraud need have "been the objective of the client's communication") and C. McCormick, McCormick on Evidence § 95, at 229 (E. Cleary 3d ed. 1984) (communication is not privileged "where the client's purpose is the furtherance of a future intended crime or fraud").

[95] 560 F.2d 326, 337 (C.A. Minn. 1977).

[96] *Id.* at 338.

> the burden of proving at least two elements. It must be established that (1) the client was engaged in or planning a criminal or fraudulent scheme when he sought the advice of counsel to further the scheme and (2) the documents containing the attorney's opinion work product must bear a close relationship to the client's existing or future scheme to commit a crime or fraud.[97]

In the insurance context, the assertion of this exception, or rather disqualification of the privilege, arises most frequently in the context of demands for the contents of the insurer's claims file in claims for bad faith. The results of these cases are mixed, but the majority view appears to be that the mere assertion of a claim for bad faith does not strip the insurer's file of protection, where warranted, of the attorney-client privilege.

In *United Services Auto. Assoc. v. Werley*,[98] though denying that the plaintiff was entitled to recover under the uninsured motorist clauses in the passengers' policies, the insurer asserted that, in the event it was held liable to the plaintiff, all the possibly interested claimants should be present to shield the insurer from double liability. In response to the insurer's interpleader action, the plaintiff filed a counterclaim for bad faith, asserting that the insurer was attempting to coerce him into accepting less than the full amount to which he was entitled under his policy.[99]

During discovery regarding his counterclaim against the insurer, Werley sought the production, in essence, of the entire claims file.[100] The insurer objected to any requested information not disclosed as protected by the attorney-client privilege. The insured filed a motion to compel which was granted by the trial court.

On review of an adverse discovery order, the appellate court held there must be a prima facie showing of fraud before the attorney-client privilege is deemed defeated. Once a litigant has presented prima facie evidence of the perpetration of a fraud or crime in the attorney-client relationship, the other party may not then claim the privilege as a bar to the discovery of relevant communications and documents.[101] The court then found that the tortuous activity alleged by the plaintiff satisfied the 'civil fraud' requirement of the exception to the attorney-client privilege. According to the court, in order to compel disclosure of attorney-client communications in cases such as this, there is not only the requirement that one allege a bad faith refusal of an insurer to pay the valid claim of its insured, but also that a prima facie case of bad faith refusal be shown.[102]

The contrary view is stated in *Dixie Mill Supply Co., Inc. v. Continental Cas. Co.*, in which the court rejected the plaintiff's demand for attorney-client communications, holding that the reasonableness of the insurers' actions in a bad faith case can be proved by objective facts, which are not shielded from discovery and do not necessarily require the introduction of privileged communications at trial.[103] The Montana Supreme Court also rejected the proposition that a claim for bad faith allows access to material protected by the attorney-client privilege. [104] the plaintiff urged the court to find there was an exception to the privilege based on other theories such as civil fraud. The court rejected the reasoning of *Escalante v. Sentry*

---

97 *Id.* at 338. *See also In re* Grand Jury Proceedings, 33 F.3d 342, 348 fn 13 (4th Cir. 1994).

98 526 P.2d 28 (Alaska 1974).

99 *Id.* at 29, 30.

100 *Id.*

101 *Id.* at 36.

102 *Id*. at 33. *See also*, State ex rel. Medical Assurance of West Virginia, Inc. v. Recht, 583 S.E.2d 80 (W. Va. 2003); Kessel v. Leavitt, 511 S.E.2d 720 (W. Va.1998).

103 Dixie Mill Supply Co., Inc., 168 F.R.D. 554, 559 (E.D. La. 1996), citing Home Indem. Co. v. Lane Powell Moss & Miller, 43 F.3d 1322, 1327 (9th Cir. 1995).

104 State ex rel. U.S. Fidelity and Guar. Co. v. Montana Second Judicial Dist., 783 P.2d 911 (Mont. 1989).

Ins.,[105] and *United Services Automobile Assoc. v. Werley*,[106] holding that those cases would extend the civil fraud exception to bad faith allegations. According to the court, the civil fraud exception to the attorney-client privilege has traditionally been invoked where an attorney or client is involved in unlawful or criminal conduct, or future fraudulent activity.[107] The court cited with approval the decision of the Florida Supreme Court in *Kujawa v. Manhattan Nat. Life Ins. Co.*[108] which held that the "legislature in creating the bad faith cause of action did not evince an intent to abolish the attorney-client privilege and work product immunity."[109]

Despite the positive citation by the Montana Supreme Court in 1989, the present state of the law in Florida is now unclear. In *Allstate Indemnity Co. v. Ruiz*,[110] the Florida Supreme Court receded from its decision in *Kujawa* and held that the work product privilege did not protect the insurer's file from discovery in a statutory first-party bad faith claim. Though the attorney-client privilege was not at issue, the court's sweeping language has arguably created some doubt whether the privilege applies to protect such communications in bad faith actions.

After the decision was entered in *Ruiz*, the Florida District Court of Appeal in *XL Specialty Ins. Co. v. Aircraft Holdings, LLC*,[111] held that, notwithstanding the expansive language in *Ruiz*, the holding in that case applied only to the work-product privilege. In reaching its decision, the court in *XL Specialty* noted the statement of Justice Wells, in his separate opinion in Ruiz: "[t]he only issue being decided in this case is the discovery of work product in the claims file pertaining to the underlying insurance claim."

The court granted the insurer's petition for writ of certiorari and quashed the trial court's order compelling attorney-client privileged documents. It then certified the following question to the Florida Supreme Court as one of great public importance:

> Does the Florida Supreme Court's holding in *Allstate Indemnity Co. v. Ruiz*, 899 So. 2d 1121 (Fla.2005), relating to discovery of work product in first-party bad faith actions brought pursuant to section 624.155, Florida Statutes, also apply to attorney-client privileged communications in the same circumstances?

We will have to await the Florida Supreme Court's pronouncement on this issue.

(E) The Parties' Respective Burdens

The person claiming the privilege bears the initial burden of establishing the applicability of the attorney-client privilege or the work product exception. The claimant must show certain threshold requirements in order to avail himself or herself of the privilege or exception including a showing that the communication originated in confidence, that it would not be disclosed, that it was made by an attorney acting in his or her legal capacity for the purpose of advising a client, and that it remained confidential. Thus, the burden of establishing the attorney-client privilege or the work product exception, in all their elements, always rests upon the person asserting it.[112] Blanket claims of privilege are not favored and the party seeking to avoid discovery has the burden of establishing the essential elements of the

---

[105] 743 P.2d 832 (Wash. 1987).

[106] 526 P.2d 28 (Alaska 1974).

[107] Citing 2 J. Weinstein, Evidence § 503(d)(1)(01.

[108] 541 So. 2d 1168 (Fla. 1989).

[109] *Id.* at 1169.

[110] 899 So. 2d 1121 (Fla. 2005).

[111] 929 So. 2d 578 (Fla. Ct. App. 2006), rev. granted, 935 So.2d 1219 (Fla. Aug 23, 2006).

[112] *See e.g.*, Ex parte CIT Communication Finance Corp., 2004 WL 1950292 (Ala. 2004); Tury v. Superior Court, 505 P.2d 1060 (Ariz. Ct. App. 1973); Gonzalez v. Superior Court, 39 Cal. Rptr. 2d 896 (Cal. App. 2 Dist. 1995).

privilege being invoked on a document-by-document basis.[113] It is well-settled that, when challenged, the proponent of the privilege must establish that the privilege was not waived.[114]

Once the privilege is established as to the material requested, in balancing the need for discovery and the need to protect the attorney's work product, the burden rests on the one who would invade that privacy to establish adequate reasons to justify production through a subpoena or court order.[115]

In the federal context, District Courts enjoy broad discretion when resolving discovery disputes, which should be exercised by determining the relevance of discovery requests, assessing oppressiveness, when weighing whether discovery should be compelled.[116] The same rule applies in state courts.[117] Given the breadth of that discretion, the appellate courts will intervene in management of pretrial discovery only upon a clear showing of manifest injustice, i.e., where the district court's discovery order was plainly wrong and resulted in substantial prejudice to an aggrieved party.[118]

Like the work-product exception, the attorney-client privilege may result in the exclusion of evidence which is otherwise relevant and material. Thus, courts are obligated to strictly construe the privilege and limit it to the purpose for which it exists.[119]

(F) Contrasting the Attorney-Client Privilege and the Work Product Doctrine

The work product doctrine, though related to the concept of attorney-client privilege, is distinct.[120] The doctrine serves a different purpose - one related to the adversary system of litigation: the protection of an attorney's private files and recorded impressions from discovery from opposing counsel.[121] Among the differences between the attorney-client privilege and the work product doctrine are: (a) the work-product doctrine may be overcome by the party seeking discovery upon a showing that production of facts in those documents is essential to the preparation of the party's case; (b) the attorney-client privilege as applied in judicial proceedings is narrowly construed, whereas the work product

---

[113] Petersen v. U.S. Reduction Co., 547 N.E.2d 860, 862 (Ind. Ct. App. 1989).

[114] Connecticut Indem. Co. v. Carrier Haulers, Inc. 197 F.R.D. 564 (W.D.N.C. 2000), citing *In re* Grand Jury Subpoena, 204 F.3d 516, 522 (4th Cir. 2000).

[115] *Id. See* also, 2,022 Ranch, L.L.C. v. Superior Court, 7 Cal. Rptr. 3d 197 (Cal. App. 4 Dist. 2003); *In re* Seigel, 198 S.W.3d 21 (Tex. Ct. App. 2006).

[116] Fed. R. Civ. P. 37, cited by Favale v. Roman Catholic Diocese of Bridgeport, 233 F.R.D. 243 (D. Conn. 2005).

[117] *See e.g.*, Ex parte Zoghby, 2006 WL 3239971 (Ala. 2006); Twin City Fire Ins. Co. v. Burke, 63 P.3d 282 (Ariz. 2003); Coleman v. PricewaterhouseCoopers, LLC, 902 A.2d 1102 (Del. 2006); Wisniewski v. Kownacki, 851 N.E.2d 1243 (Ill. 2006); *In re* City of Wichita, 86 P.3d 513 (Kan. 2004); Bugger v. McGough, 144 P.3d 802 (Mont. 2006); McNeil v. McNeil, 2006 WL 709115 (Pa. 2006); T.S. v. Boy Scouts of America, 2006 WL 2104204 (Wash. 2006).

[118] U.S. Steel v. M. DeMatteo Const. Co., 315 F.3d 43 (1st Cir. 2002).

[119] Upjohn Co. *supra*; State v. Smith, 50 S.E. 859, 860 (1905); Fisher v. United States, 425 U.S. 391, 403 (1976); E.I. du Pont de Nemours & Co. v. Forma-Pack, Inc., 718 A.2d 1129 (Md. 1998); Delta Financial Corp. v. Morrison, 820 N.Y.S.2d 745 (N.Y. Supp. 2006). *See also In re* Shargel 742 F.2d 61, 62 (2d Cir. 1984); *In re* Special, September 1983, Grand Jury (Klein), 608 F.Supp. 538, 542, *aff'd*, 776 F.2d 628 (S.D. Ind. 1985); 8 John H. Wigmore, Evidence § 2291, at 554 (McNaughton rev. ed. 1961).

[120] Pratt v. State, 387 A.2d 779, 782 n. 2 (Md. Ct. App. 1978). *See also* John F. Wagner, Jr., Protection from Discovery of Attorney's Opinion Work Product Under Rule 26(B)(3), Federal Rules of Civil Procedure, 84 ALR Fed. 779 (1987).

[121] Hercules Inc. v. Exxon Corp., 434 F. Supp. 136, 150 (D.N.J. 1976).

doctrine is broader in scope;[122] and, (c) the work product privilege may be asserted by either the client or the attorney.[123]

As some courts have noted, the work product privilege may not be a privilege at all, but "merely a requirement that very good cause be shown if the disclosure is made in the course of a lawyer's preparation of a case."[124] If it is a privilege, the work product doctrine is "historically and traditionally a privilege of the attorney and not that of the client."[125] In contrast, it is the client who is the holder of the attorney-client privilege.[126]

IV. The Work Product Doctrine

The federal work product doctrine was established in *Hickman v. Taylor*.[127] In rejecting the plaintiff's demand for statements and other work product, the court noted that the proper preparation of a client's case demands that the attorney assemble information, sift what he or she considers to be the relevant from the irrelevant facts, prepare legal theories and plan his or her strategy without undue and needless interference. The attorney's work is reflected in interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs, and countless other tangible and intangible ways-aptly termed as attorney work product. The effect on the legal profession of opening that work product up to opposing counsel would be demoralizing and the interests of the client and the cause of justice would be poorly served.[128]

The central purpose of the work-product doctrine is to protect the mental processes of the attorney from discovery, providing a privileged area within which he or she can analyze and prepare the client's case. But, as the Supreme Court noted in U.S. v. Nobles,[129] "the doctrine is an intensely practical one, grounded in the realities of litigation in our adversary system. One of those realities is that attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial. It is therefore necessary that the doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself."[130]

The work product doctrine is now expressed in Rule 26(b)(3), Federal Rule of Civil Procedure, and the state court rules that have adopted it. The work-product rule enunciated in *Hickman* was expanded by subsection (b)(3) specifically to cover trial preparation materials of non-lawyers.[131] This expansion of the application of the restrictive work-product doctrine, however, applies by the terms of the Rule when the materials requested for production were

---

[122] E.I. du Pont de Nemours & Co. v. Forma-Pack, Inc., 718 A.2d 1129 (Md. 1998).

[123] Edward J. Krauland and Troy H. Cribb, The Attorney-Client Privilege in the United States - An Age-Old Principle under Modern Pressures, 2003 Prof. Law. 37 (2003).

[124] City of Philadelphia v. Westinghouse Elec. Corp., 210 F.Supp. 483, 485 (E.D. Pa. 1962).

[125] Radiant Burners, Inc. v. American Gas Association, 207 F.Supp. 771, 776 (N.D. Ill. 1962).

[126] Trupp v. Wolff, 335 A.2d 171, 184 (Md. Ct. Spec. App. 1975).

[127] 329 U.S. 495 (1947).

[128] *Id.* at 511.

[129] 422 U.S. 225 (1975).

[130] *Id.* at 238.

[131] U.S. v. Nobles, *supra*, at fn 13. The plain language of the rule does not require that an attorney be involved in the preparation of the material. *See* 8 C. Wright & A. Miller, Federal Practice & Procedure § 2024, at 205-07 (1970); Toledo Edison Co. v. G.A. Technologies, Inc., 847 F.2d 335 (6th Cir. 1988); Duplan Corp. v. Deering Milliken, Inc., 540 F.2d 1215, 1219 (4th Cir. 1976); Scott Paper Co. v. Ceilcote Co., 103 F.R.D. 591, 594 (D. Me. 1984); Thomas Organ Co. v. Jadranska Slobodna Plovidba, 54 F.R.D. 367, 370 (N.D. Ill. 1972); Hawkins v. District Court, Fourth Judicial Dist., 638 P.2d 1372, 1376-77 (Colo. 1982); Gold Standard, Inc. v. American Barrick Resources Corp. 805 P.2d 164 (Utah 1990).

prepared in anticipation of litigation or for trial.[132]

The Rule provides that documents "prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative" may be obtained in discovery "only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means."[133] Thus, under the plain language of the rule, there are two kinds of work product with differing standards of protection: ordinary work product and opinion work product. In *Baker v. General Motors Corp.*,[134] the Eighth Circuit Court of Appeals explained the difference between them as follows:

> Ordinary work product includes raw factual information. *See Gundacker v. Unisys Corp.*, 151 F.3d 842, 848 n. 4 (8th Cir.1998). Opinion work product includes counsel's mental impressions, conclusions, opinions or legal theories. *See Id.* at n. 5. Ordinary work product is not discoverable unless the party seeking discovery has a substantial need for the materials and the party cannot obtain the substantial equivalent of the materials by other means. *See* Fed. R. Civ. P. 26(b)(3). In contrast, opinion work product enjoys almost absolute immunity and can be discovered only in very rare and extraordinary circumstances, such as when the material demonstrates that an attorney is engaged in illegal conduct or fraud. *See In re Murphy*, 560 F.2d 326, 336 (8th Cir. 1977). [135]

The primary reasons for the protection given by the work product doctrine to materials prepared in anticipation of litigation are to maintain the adversarial trial process and to ensure that attorneys are properly prepared for trial by encouraging written preparation.[136] Attorneys should not be deterred from adequately preparing for trial because of fear that the fruits of their labors will be freely accessible to opposing counsel.[137] Finally, allowing discovery of work product could lead to a party's attorney being called as a witness.[138]

(A) The Origin and Nature of the Doctrine's Balancing Test

Balanced against the importance of protecting work product is the fundamental consideration that procedural rules should be construed to allow discovery of all relevant information in order to facilitate a trial based on the true and complete issues.[139] Because work product protection by its nature may hinder an investigation into facts relevant to the issues before the court, it should be narrowly construed consistent with its purpose, which is to

---

[132] Thomas Organ Co., *supra*.

[133] Fed. R. Civ. P. 26(b)(3).

[134] 209 F.3d 1051, 1054 (8th Cir. 2000).

[135] *Id.*, citing *In re* Murphy, 560 F.2d 326 (8th Cir. 1977). *See also* Haney v. Yates, 40 S.W.3d 352 (Ky. 2000) (documents containing the mental impressions or legal conclusions of an attorney are absolutely privileged); Limstrom v. Ladenburg, 963 P.2d 869 (Wash. 1998) (notes or memoranda prepared by an attorney from oral communications should be absolutely protected under the work product rule, unless the attorney's mental impressions are directly at issue); Hull Mun. Lighting Plant v. Massachusetts Mun. Wholesale Elec. Co., 609 N.E.2d 460 (Mass. 1993) (order must protect against disclosure of mental impressions, conclusions, opinions or legal theories of attorney or other representative of party concerning litigation); Richey v. Chappell, 594 N.E.2d 443 (Ind. 1992) (even with a showing that the claimant is unable, without undue hardship, to obtain the substantial equivalent by other means of hardship, party seeking discovery is in no event entitled to mental impressions, conclusions, opinions, or legal theories of attorney or other representative of party concerning litigation).

[136] Hickman, *supra* at 510-12.

[137] Hickman, *supra* at 511.

[138] Hickman, *supra* at 517 (Jackson, J., concurring).

[139] Hickman, *supra* at 507.

"safeguard the lawyer's work in developing his client's case."[140]

(1) The Three Prong Test of Rule 26(b)(3) FRCP

Rule 26(b)(3) sets out a three-prong test to determine whether matter is to be characterized as ordinary (not opinion) work product. The party asserting work product privilege bears the burden of showing (1) that the material consists of documents or tangible things, (2) which were prepared in anticipation of litigation or for trial, and (3) by or for another party or its representatives.[141] Much of the litigation regarding the contents of the insurer's claims file addresses the second prong, i.e., whether the material was in fact created in anticipation of litigation.

(2) The Parties' Respective Burdens

As in the case of the attorney-client privilege, the burden to demonstrate that the matter being sought is indeed work-product as defined by Rule 26(b)(3) is upon the party resisting discovery.[142] Once an insured moves to compel the production of the documents in an insurer's claims file, the burden shifts to the insurer to establish that the requested documents were generated in anticipation of litigation and are thus protected by the work-product privilege.[143] Unless that party establishes that the privilege should attach, discovery of the requested documents will be permitted.[144] Even where the material qualifies as ordinary work product, discovery of that material will be granted when the party seeking discovery demonstrates a "substantial need" for the document and "undue hardship" in obtaining its substantial equivalent by other means.[145]

Where the material sought consists of opinion work product, items containing the "mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation" the material can only be discovered when the party seeking discovery establishes extraordinary circumstances, such as when the material demonstrates that an attorney engaged in illegal conduct or fraud.[146]

As in the case of other matters protected by privilege, the protection provided by the work-product doctrine is not absolute, and it may be waived.[147] Under the so called "waiver doctrine," voluntary disclosure of work product to an adversary waives privilege as to other parties.[148] The cases are mixed on whether inadvertent disclosure waives the privilege.[149] Some cases have said that, as the work product privilege, unlike attorney-client privilege, does not exist to protect a confidential relationship but to promote the adversary system by safeguarding the fruits of an attorney's trial preparation from discovery attempts of an opponent, disclosure of work product to a third party does not waive its protection unless it

---

[140] Evans, *supra*, citing Suggs v. Whitaker, 152 F.R.D. 501, 505 (M.D.N.C. 1993).

[141] *Id.,* citing Sandberg v. Virginia Bankshares, Inc., 979 F.2d 332, 355 (4th Cir. 1992).

[142] Sham v. Hyannis Heritage House Hotel, Inc., 118 F.R.D. 24 (D. Mass. 1987); *In Re* BP Products North America Inc., ---S.W.3d----, 2006 WL 2973037 (Tex. Ct. App. 2006).

[143] Ex parte State Farm Mut. Auto. Ins. Co., 761 So. 2d 1000 (Ala. 2000).

[144] Redvanly v. NYNEX Corp., 152 F.R.D. 460 (S.D. N.Y. 1993).

[145] E.I. du Pont de Nemours & Co. v. Forma-Pack, Inc., 718 A.2d 1129 (Md. 1998).

[146] Baker, *supra,* citing *In re* Murphy, 560 F.2d 326, 336 (8th Cir. 1977) and Juneau v. Avoyelles Parish Policy Jury, 482 So. 2d 1022 (La. Ct. App. 1986).

[147] *In re* Qwest Communications Intern. Inc., 450 F.3d 1179 (10th Cir. 2006). *See also* State ex rel. Ford Motor Co. v. Westbrooke, 2004 WL 2663647 (Mo. 2004).

[148] *In re* Steinhardt Partners, L.P., 9 F.3d 230 (2d Cir. 1993).

[149] *See* Mendenhall v. Barber-Greene Co., 531 F.Supp. 951, 954 (N.D. Ill. 1982) (the better-reasoned rule is that mere inadvertent production does not waive the privilege).

substantially increases the opportunity for potential adversaries to obtain the information.[150] Others have held that, where disclosure of privileged documents is inadvertent rather than a knowing waiver, discovery of the material will not be ordered.[151]

The majority view appears to be a middle ground stated by the court in *Hydraflow, Inc. v. Enidine Inc.*[152] Under the *Hydraflow* test, the court should undertake a five-step analysis of the unintentionally disclosed document to determine the proper range of privilege to extend. These considerations are (1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of document production, (2) the number of inadvertent disclosures, (3) the extent of the disclosures, (4) the promptness of measures taken to rectify the disclosure, and (5) whether the overriding interest of justice would be served by relieving the party of its error.[153]

(3) State Law

As noted above, a majority of states have adopted the work product protections of Rule 26 of the Federal Rules. For the most part, they have interpreted the state versions of Rule 26 with reference to interpretations by the federal courts.[154]

(B) In Anticipation of Litigation

The question of whether particular material was prepared in "anticipation of litigation" has proven to be a major source of disagreement between the Federal Courts. Insurers assert the work product doctrine to protect reports, memorandum and investigations made by their representatives after an accident. Such materials are undoubtedly created with an eye towards possible, and, depending on the severity of the incident giving rise to the claim, even highly likely, litigation. In spite of this reality, the conflicting judicial decisions center on the question of whether the work product doctrine embodied in Rule 26(b)(3) was intended to provide these materials broad privilege from discovery because of the *possibility* that litigation would ensue as a result of the claims which precipitate the insurer's investigation.

In the context of insurance litigation, determining whether a document was created in anticipation of litigation is particularly challenging because the very nature of the insurer's business is to investigate claims. Because insurance companies regularly investigate claims, such investigations would normally seem to be in the ordinary course of business rather than in anticipation of litigation.[155] Although it seems clear that the possibility of litigation exists from the denial of any claim, the courts generally have held that statements or reports made by parties and their employees in the regular course of business are not work-product and should be produced for discovery when so requested by the opposing party.[156]

---

[150] Shields v. Sturm, Ruger & Co., 864 F.2d 379 (5th Cir. 1989).

[151] Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103 (S.D.N.Y. 1985).

[152] 145 F.R.D. 626 (W.D.N.Y. 1993).

[153] *Id.* at 378. For a list of state and federal cases adhering to the Hydraflow approach, *see* State ex rel. Allstate Ins. Co. v. Gaughan, 508 S.E.2d 75, 94 fn 40 (W. Va. 1998).

[154] *See* Columbia/HCA Healthcare Corp. v. Eighth Judicial Dist. Court In and For County of Clark, 936 P.2d 844 (Nev. 1997) ("[E]ven though litigation is already in prospect, there is no work product immunity for documents prepared in the regular course of business rather than for purposes of litigation."); Wells Dairy, Inc. v. American Indus. Refrigeration, Inc., 690 N.W.2d 38 (Iowa 2004); Springfield Terminal Ry. Co. v. Department of Transp., 754 A.2d 353 (Me. 2000).

[155] *See* M. Elizabeth Medaglia, et al., Privilege, Work Product, and Discovery Issues in Bad Faith Litigation, 32 Tort & Ins. L.J. 1, 12 (1996), cited by Evans v. United Services Auto. Assoc., 541 S.E.2d 782 (N.C. Ct. App. 2001).

[156] *See* Burns v. New York Central R. Co., 33 F.R.D. 309, 310 (N.D. Ohio 1963); United States v. Swift & Co., 24 F.R.D. 280, 282 (N.D. Ill. 1959); Morrone v. Southern Pacific Co., 7 F.R.D. 214, 215 (S.D. Cal. 1947); Durkin v. Pet Milk Co., 14 F.R.D.

Courts are split on what standard to apply to determine whether a document has been created in anticipation of litigation and not in the ordinary course of business. The most troublesome area has been where the documents are prepared by non-lawyer investigators and adjusters before counsel is engaged by the insurer. Some courts have held that attorney involvement is required.[157] Other courts have held the opposite position, one that presumes that such reports were made in anticipation of litigation.[158] A third group of courts rejected both approaches and have viewed attorney involvement as only one factor in a more fact-specific determination of whether material was prepared in anticipation of litigation.[159]

(1) Presumption of Ordinary Course of Business

In *Thomas Organ Co. v. Jadranska Slobodna Plovidba*,[160] the court held that neither the transcription of dictation made by a marine surveyor hired by the insurer nor a letter from that surveyor, based in part on the dictation, could be considered as prepared in anticipation of litigation or for trial. The trial court noted that the documents might contain the surveyor's impressions, conclusions, and opinions. It also noted that the documents were prepared because of specific claims that had already arisen and that litigation was an identifiable contingency at the time of preparation. However, the documents were prepared months before the insurer paid the claim, received the subrogation agreement from the insured or caused suit to be instituted. Perhaps more importantly, the documents were prepared months before the attorney first became involved. As a consequence, the court held that both documents, being relevant, were discoverable without any showing of need.[161]

(2) Presumption Against Ordinary Course of Business

A second group of courts has taken the position that documents prepared by non-lawyer agents of the insurer immediately following an accident are indeed made in anticipation of litigation. This interpretation of the rule, enunciated by the Maine Supreme Court in *Harriman v. Maddocks* offers insurance claim files broad protection from disclosure under the work-product doctrine.[162]

In *Harriman*, the plaintiffs filed a motion for discovery of the entire case file compiled by the insurer's adjuster. The trial court conducted an in-camera inspection, separating documents on the basis of whether they were relevant and, if relevant, determined whether they were nonetheless protected as work product. On appeal, the plaintiffs asserted that the court should have permitted discovery of the adjuster's entire file, assuming relevance, without requiring

---

385, 391-394 (W.D. Ark. 1953); California v. United States, 27 F.R.D. 261, 262 (N.D. Cal. 1961); Burke v. United States, 32 F.R.D. 213, 214-215 (E.D.N.Y. 1963); Newell v. Capital Transit Co., 7 F.R.D. 732, 734 (D.D.C. 1948); Herbst v. Chicago, R.I. & P.R. Co., 10 F.R.D. 14, 18-19 (S.D. Iowa 1950); Szymanski v. New York, N.H. & H. R.R., 14 F.R.D. 82, 83 (S.D.N.Y. 1952); Brown v. N.Y., N.H. & H. R.R., 17 F.R.D. 324, 325 (S.D.N.Y. 1955).

[157] McDougall v. Dunn, 468 F.2d 468 (4th Cir. 1972); Langdon v. Champion, 752 P.2d 999 (Alaska 1988); Henry Enterprises, Inc. v. Smith, 592 P.2d 915 (Kan. 1979).

[158] Fireman's Fund Ins. Co. v. McAlpine, 391 A.2d 84 (R.I. 1978). *See also* Basinger v. Glacier Carriers, Inc., 107 F.R.D. 771, 773 (M.D. Pa. 1985), citing Fontaine v. Sunflower Beef Carrier, 87 F.R.D. 89 (E.D. Mo. 1980) and Almaguer v. Chicago, Rock Island & Pacific R.D., 55 F.R.D. 147 (D. Neb. 1972).

[159] Moore v. Tri-City Hosp. Auth., 118 F.R.D. 646 (N.D. Ga. 1988); Basinger v. Glacier Carriers, Inc., 107 F.R.D. 771, 773-74 (M.D. Pa. 1985); Scott Paper Co. v. Ceilcote Co., 103 F.R.D. 591, 594 (D. Me. 1984); APL Corp. v. Aetna Casualty & Sur. Co., 91 F.R.D. 10, 18 (D. Md. 1980); Spaulding v. Denton, 68 F.R.D. 342, 345 (D. Del. 1975).

[160] Thomas Organ Co., *supra.*

[161] *Id.*

[162] 518 A.2d 1027 (Me. 1986).

the plaintiffs to make any showing that the materials in the file were not prepared in anticipation of litigation, nor of a substantial need for the materials. In rejecting the claim of the plaintiffs, and citing the criticism of *Thomas Organ Co.*, the court advised there was no distinction between materials prepared by an attorney and those that are prepared by a claim agent. Therefore, the involvement of an attorney is not a prerequisite to the application of Rule 26(b)(3).[163]

(3) The Case by Case Method

The so call "case-by-case" method appears to be the majority rule on whether documents created by non-lawyer inspectors and adjusters who are not under the direction of an attorney are nonetheless entitled to work product protection.[164] Under this rule, adopted by the court in *State Farm Fire & Cas. Co. v. Perrigan*,[165] whether the claims materials demanded by the plaintiff are subject to discovery depends upon the facts of each case.[166] The test in the case-by-case method is whether, in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation. As under the other tests, there is no work product immunity for documents prepared in the regular course of business (rather than for purposes of litigation) even though litigation is already contemplated, pending or even in progress.[167]

The advantage of the case by case approach is that it acknowledges that, at some point, an insurer must necessarily shift the focus of its activity from the ordinary course of business to litigation. As a practical matter, this shift in focus occurs at different times in different cases. Rejecting the idea that some blanket presumption can accurately govern when the shift occurs,[168] this method recognizes the factual differences in cases and focuses on that pivotal point where the probability of litigating the claim is substantial and imminent.[169] Some courts defined the factual inquiry as whether litigation was reasonably foreseeable at the time the requested document was prepared.[170]

(C) The Good Cause/Undue Hardship Doctrine

The basis for the "good cause" exception to the protection for otherwise privileged work product is Rule 26. In *Hickman v. Taylor*,[171] the Supreme Court denied the plaintiff's demand for an attempt to obtain work product holding that such discovery "without purported necessity or

---

[163] *Id.* at 1033.

[164] *See* S.D. Warren Co. v. Eastern Elec. Corp., 201 F.R.D. 280 (D. Me. 2001). *See also* Ex parte Cummings, 776 So. 2d 771 (Ala. 2000); Wells Dairy, Inc. v. American Indus. Refrigeration, Inc., 690 N.W.2d 38 (Iowa 2004); Springfield Terminal Ry. Co. v. Department of Transp., 754 A.2d 353 (Me. 2000); Heffron v. District Court Oklahoma County, 77 P.3d 1069 (Okla. 2003); State of West Virginia Ex Rel. Allstate Ins. Co. v. Madden, 2004 WL 1144057 (W. Va. 2004); Lane v. Sharp Packaging Systems, Inc., 640 N.W.2d 788 (Wis. 2002).

[165] 102 F.R.D. 235, 238 (W.D. Va. 1984).

[166] Carver v. Allstate Ins. Co., 94 F.R.D. 131, 134 (S.D. Ga. 1982); Spaulding v. Denton, 68 F.R.D. 342, 345-46 (D. Del. 1975); American Home Assurance Co. v. Libbey-Owens-Ford Co., 37 Fed. R. Serv. 628, 632 (D. Mass. 1983).

[167] Hercules, Inc. v. Exxon Corp., 434 F.Supp. 136, 151 (D. Del. 1977); Miles v. Bell Helicopter Co., 385 F.Supp. 1029, 1032-33 (N.D. Ga. 1974); Hi-G Incorporated v. Insurance Co. of North America, 35 Fed. R. Serv. 861, 862 (D. Mass. 1982). *See also*, 8 C. Wright & A. Miller, Federal Practice & Procedure: Civil § 2024 at 198-99 (1970).

[168] Westhemeco Ltd. v. New Hampshire Insurance Co., 82 F.R.D. 702, 708 (S.D. N.Y. 1979).

[169] Carver v. Allstate Ins. Co., 94 F.R.D. 131, 134 (S.D. Ga. 1982), citing APL Corp. v. Aetna Casualty & Surety Co., 91 F.R.D. 10, 21 (D. Md. 1980); Klawes v. Firestone Tire & Rubber Co., 572 F.Supp. 116, 125 (E.D. Wis. 1983).

[170] Coastal States Gas Corp. v. Department of Energy, 617 F.2d 854, 865 (D.C. Cir. 1980).

[171] Hickman, *supra*.

justification" fell outside the arena of discovery and contravenes the public policy underlying the orderly prosecution and defense of legal claims.[172] Under the plain language of Rule 26, a finding that the material demanded by a litigant falls within the work product privilege does not mean that the court will not order it produced. To obtain otherwise protected material, the claimant will have to show "good cause." Good cause will necessarily depend upon the facts of the individual case and, therefore, is not susceptible to a single definition.

Certainly the mere assertion that discovery is necessary for a movant to investigate fully and prepare his case is insufficient as a statement of good cause warranting order for production of documents.[173] As the *Fulcher* court advised, "There must instead be some special circumstances in addition to relevancy. The discovery procedures were not intended to open an attorney's files to opposing counsel; nor were they intended to afford an attorney the luxury of having opposing counsel investigate his case for him."[174]

While good cause has been interpreted in differing ways,[175] in general the claimant will have to show an inability to secure the substantial equivalent of the materials by alternate means without undue hardship.[176] What hardship is "undue" depends on both the alternative means available and the need for continuing protection from discovery.[177] Discovery has also been allowed where crucial information was in the exclusive control of the opposing party.[178] On the other hand, the good cause requirement is not met if the discovering party merely wants to be sure nothing has been overlooked or merely hopes to unearth damaging admissions.[179]

Apart from those cases where the evidence sought is only to be had from the opposite party, the focus of litigation will usually focus on whether the alternatives available to the person seeking discovery are substantially equivalent. Where both parties have an equal opportunity to investigate, and where all the witnesses to the accident are known and available to both sides, discovery should not be granted.[180]

With respect to the insurer's claims file, the good cause issue frequently arises in connection with demands for statements taken by the insurer's investigators or counsel. As noted above during the discussion of the expected contents of the claims file, such statements have been found to be protected as work product. The special nature of such statements, however, frequently results in their production despite the work product privilege. The reason for such treatment was stated by the court in *Fireman's Fund Ins. Co. v. McAlpine*.[181] The court noted that such statements taken

---

[172] Hickman, *supra*, at 510.

[173] 172 S.E.2d 751 (Va. 1970).

[174] *Id.*

[175] One commentator has advanced the following general test for good cause: Generally speaking, however, it was held that the moving party must demonstrate that inspection of documents to be produced is in some way necessary to the adequate preparation of its case . . . In short, any showing that failure to order production would unduly prejudice the preparation of the party's case, or cause him hardship or injustice, would support the order. 4A Moore's Fed. Prac. § 34.08 (1974), cited by Stanback v. Stanback, 287 N.C. 448, 215 S.E.2d 30 (N.C. 1975).

[176] *See* Chaudhry v. Gallerizzo, 174 F.3d 394, 403 (4th Cir. 1999), quoting In re Grand Jury Proceedings, 33 F.3d 342, 348 (4th Cir. 1994); State ex rel. Medical Assurance of West Virginia, Inc. v. Recht, 583 S.E.2d 80 (W. Va. 2003).

[177] State ex rel. Chaparro v. Wilkes, 438 S.E.2d 575, 578 fn 2 (W. Va.1993).

[178] *See* Loctite Corp. v. Fel-Pro, Inc., 667 F.2d 577 (7th Cir. 1981); State ex rel. Medical Assurance of West Virginia, Inc. v. Recht, 583 S.E.2d 80 (W. Va. 2003).

[179] Republic Gear Co. v. Borg-Warner Corp., 381 F.2d 551, 557 (2d Cir. 1967); Alltmont v. United States, 177 F.2d 971 (3d Cir. 1949), cert. denied, 339 U.S. 967 (1950).

[180] Rakes v. Fulcher, 172 S.E.2d 751, citing Koss v. American S.S. Co., 27 F.R.D. 511, 512 (E.D. Mich. 1960); Herrick v. Barber S. S. Lines, Inc., 41 F.R.D. 51, 52 (S.D.N.Y. 1966).

[181] 391 A.2d 84 (R.I. 1978).

immediately after an event "are unique catalysts in the search for truth in that they provide an immediate impression of the facts, the substantial equivalent of which cannot be recreated or duplicated by a deposition or interview months or years after the event."[182] According to the court, the unique quality of such statements has been determined to provide special circumstances satisfying the undue hardship requirement needed to overcome their protection as work product.[183]

Some of the factors to consider in the case of witness statements were outlined by the West Virginia Supreme Court in *State ex rel. Medical Assurance of West Virginia, Inc. v. Recht.*[184] In *Recht*, the court held the "substantial need" and "undue hardship" standard is met where 1) a witness is no longer available for questioning, 2) a witness is hostile and refuses to give a statement, or 3) the witness has a faulty memory and can no longer remember the details of the event in question.[185] Similar considerations have been used as the basis to order the production of an accident report containing the opinions of the investigator.[186] Other cases have held that the availability of the witnesses whose statements are sought obviates a finding of good cause.[187]

(D) Waiver in Case of "Bad Faith"

As in claims for materials protected by the attorney-client privilege, plaintiffs frequently assert that documents covered by the work product privilege lose that protection when the cause of action is for bad faith. As noted above, some states, like Florida, have found that such materials must be produced in bad faith cases.[188] However, other courts have rejected that broad brush approach.

In *State ex rel. U.S. Fidelity and Guar. Co. v. Montana Second Judicial Dist.*,[189] the Montana Supreme Court noted that the civil fraud exception to the attorney-client privilege has traditionally been invoked where an attorney or client is involved in unlawful or criminal conduct, or future expected fraudulent activity. It rejected the reasoning of cases that would extend the civil fraud exception to bad faith allegations.[190]

Other courts have compelled the production of the insurer's claims file but done so using the familiar standards for factual (rather than opinion) work product. For example, in *Prisco Serena Sturm Architects, Ltd. v. Liberty Mut. Ins. Co.*,[191] the court compelled production of the claims file noting that "[t]he claims file is a unique, contemporaneously prepared history of the company's handling of the claim; in an action such as this the need for the information in the file is not only substantial, but overwhelming. ... It follows that where allegations of bad faith exist against an insurance company, the plaintiff insured is entitled to know the substance of the investigation, the information available and used to make a decision, and the

---

[182] *Id.* at 775.

[183] *Id.* citing McDougall v. Dunn, 468 F.2d 468 (4th Cir. 1972); Southern Railway Co. v. Lanham, 403 F.2d 119 (5th Cir. 1968); Teribery v. Norfolk & Western Railway, 68 F.R.D. 46 (W.D. Pa. 1975); Tiernan v. Westext Transport Inc., 46 F.R.D. 3 (D. R.I. 1969); Johnson v. Ford, 35 F.R.D. 347 (D. Colo. 1964); DeBruce v. Pennsylvania R. Co., 6 F.R.D. 403 (E.D. Pa. 1947); Tinder v. McGowan, 15 F.R. Serv. 2d 1608 (W.D. Pa. 1970).

[184] 583 S.E.2d 80 (W. Va. 2003).

[185] *See also* Carmen v. Fishel, 418 P.2d 963, 972 (Okl. 1966)

[186] Ogea v. Jacobs, 344 So. 2d 953 (La. 1977). Cf. Holmes v. Gardler, 62 F.R.D. 70 (E.D. Pa. 1974) and Frankenhauser v. Rizzo, 59 F.R.D. 339 (E.D. Pa. 1973) (the court approved the redaction of opinions contained within factual reports).

[187] See Uncle Ben's, Inc. v. Uncle Ben's Pancake Houses, Inc., 30 F.R.D. 506 (S.D. Tex. 1962); Richards v. Maine Central Rd., 21 F.R.D. 593 (D. Me. 1957); Goldner v. Chicago & N.W. Ry. System, 13 F.R.D. 326. (N.D. Ill. 1952).

[188] Ruiz, *supra*.

[189] 783 P.2d 911 (Mont. 1989).

[190] *Id.*, citing 2 J. Weinstein, Evidence § 503(d)(1)(01); Annot., 31 ALR 4th 45.

[191] 1996 WL 89225, 1 (N.D. Ill. 1996).

evaluations and advice relied upon for the decision."[192]

Still other courts have held the plaintiff in bad faith cases to a stronger showing of good cause. For example, the court in *Ring v. Commercial Union Ins. Co.*,[193] declined to order production of the insurer's claims file because the cause of action involved bad faith. The court noted "[w]hile arguably it may be more difficult to prove a claim of bad faith, failure to settle without examining an insurance company's claims file, does not mean it is impossible." According to the court, the plaintiff could "thoroughly depose and examine the defendants' adjuster to find out all of his actions and decisions leading to the denial of the claim."[194]

V. Conclusion

As the cases above demonstrate, broad requests for the insurer's claims file are objectionable. A blanket request for the entire claims file is not sufficiently detailed to permit the parties and the court to understand with certainty the nature of the documents demanded. Instead, the request must be defined with sufficient particularity to enable the opposing party to interpose the grounds of objection it may have to the requested production. In addition, the request must sufficiently describe the documents sought to enable the Court to intelligently rule on the opposing party's objections.

In the insured's suit against the insurer following a coverage decision, demand for many of the items within the insurer's claims file will fail on grounds of relevance. While the standard for relevance under state and federal rules is broad, the material requested must either make a fact at issue more or less likely than it would be without the requested material or reasonably lead to such material. The typical contents of the insurer's file, such as internal communications and memoranda, and materials related to internal procedures and policies such as directives, guidelines and manuals, are simply not relevant to the actual facts at issue, the nature of the damage claimed, or the nature of the peril that the insured alleges resulted in the damage claimed.

The other portions of the insurer's claims file, i.e., entries in a claims diary or log, reports by outside investigators, and materials generated by the insurer's personnel and outside investigators, including statements taken from potential witnesses, are frequently subject to the attorney-client and work product privileges. While the insurer must satisfy the court that each document meets the elements of one of these privileges, the mere fact that such material is relevant or even essential to the success of the plaintiff's case does not mean the court can order its production.

Finally, while some jurisdictions have granted wide exceptions to the work product privilege in bad faith litigation, a blanket waiver of the work product privilege in bad faith cases is not the rule. Even here, the plaintiff bears the burden of showing relevance and, if the privilege is deemed to apply, good cause to obtain the material. In most jurisdictions, this will mean a showing that the material cannot be obtained without hardship from any other source.

---

[192] *Id.* at 1. Other courts have concurred with this result. *See, e.g.*, Silva v. Fire Ins. Exchange, 112 F.R.D. 699 (D. Mont. 1986); Brown v. Superior Court In and For Maricopa County, 670 P.2d 725, 734 (Ariz. 1983); Pete Rinaldi's Fast Foods, Inc. v. Great American Ins. Companies, 123 F.R.D. 198, 203 (M.D.N.C. 1988); Holmgren v. State Farm Mut. Auto. Ins. Co., 976 F.2d 573, 577 (9th Cir. 1992);Transport Insurance Company, Inc. v. Post Express Company, Inc., 1996 WL 32877, 3 (N.D. Ill. 1996) (in finding a substantial need, the court compelled production of the file because the claims file sought was "the only record of how Transport handled the claim and, therefore, the only evidence on whether Transport acted reasonably or in good faith in failing to settle the claim against Post Express in the [insured's] lawsuit.").

[193] 159 F.R.D. 653, 658 (M.D.N.C. 1995). *See also* Bartlett v. State Farm Mut. Auto. Ins., 206 F.R.D. 623 (S.D. Ind. 2002).

[194] *Id.*

As noted at the beginning of this article, in the current environment, discovery in individual cases is increasingly a vehicle for the collection of evidence to be studied, shared and used to build later cases against the defendant by large plaintiffs' firms or affiliated plaintiffs' counsel in other jurisdictions. It will be for the insurer's counsel to protect her clients by ensuring that disclosures in individual cases are limited, as much as possible, to the proper discovery relevant to the facts at issue in the individual case before the court.

The Privacy Project III

Confidential Settlements: Issues for Consideration

By: William B. Crow

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 liability litigation, and insurance coverage issues.

The last time we considered settlement agreements and their claimed or desired confidentiality, we discussed the "Sunshine Acts" of various states, the difficulty of keeping court filed agreements confidential, and other related problems.[1] In the end we concluded, among other things, that if you or your client truly desire confidentiality, you should not depend on the court to preserve it. In sum, if you want a settlement agreement kept confidential, keep it private; don't file it with the court if it can be prevented. The odds are that if the settlement agreement is not filed with the court, it is likely to remain confidential.

Sealed settlement agreements, however, have become increasingly more vulnerable to public disclosure as some lawyers (from the dark side), and to a greater extent the media, continue to promote the Sunshine Acts.[2] The arguments in favor of the Sunshine Acts generally are presented on the claim of right of the public to know, but just as frequently, we suspect, are made for more mischievous purposes, such as the desire to embarrass one of the litigants.

Here we will consider different scenarios, the application of certain common provisions of the Sunshine Acts, and the advantages or disadvantages of having certain settlement agreements filed with the court under seal. Further, we will explore the sometimes troubling legal and ethical questions that can arise when a sealed settlement is contemplated by the parties.

Consider:

1. Your client is the Archbishop of the local Archdiocese. One, then two, and then a number of claims are made against the Archdiocese alleging child (usually sexual) abuse by a living priest. The parties reach a settlement. Plaintiff wants the settlement kept confidential for privacy reasons (usually to prevent embarrassment), and defendant wants to maintain confidentiality for a variety of reasons. Is it appropriate to seek confidentiality if it may mean exposure of others to similar abuse? Is plaintiff's desire to remain anonymous significant? Does removal of the priest from contact with children have any effect? What is your responsibility as a lawyer—to your client—to the public? Do any doubts as to truthfulness of the claims matter?

---

[1] William B. Crow, 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, The Privacy Project, Phase II (Int'l Assn. Def. Counsel Feb. 2004). The author of this article would also like to give credit and a special thanks to Christiane Fife, without whom the article would not have happened.

[2] These Acts generally take the form of a state statute, rule of civil procedure, or local court rule and provide for a range of restrictions on confidential settlement agreements filed with the court. The most extreme being a total ban on the court's sealing of settlements. *See* S.C. Fed. Dist. Ct. L. Civ. R. 5.03(c). Most provide that a court may seal settlements either when good cause is shown or when the agreement will not conceal a public hazard or information related to a public hazard. *See e.g.*, N.Y. CLS Unif. R. Tr. Cts. § 216.1; Fla. Stat. § 69.081; Tex. R. Civ. P. 76a.

2. Do the responsibilities change if your client is instead a school district? What if this is the only claim ever asserted against this teacher and you doubt its truthfulness? If it is kept confidential, what is the advice you give your client if the teacher seeks a job at another school? Does your advice change if you believe the allegations?

3. Suppose that a particular plaintiff's lawyer continues to make an excellent living by bringing one lawsuit after similar lawsuit against your client. Can you reach a confidential settlement agreement providing a bonus if the lawyer will stop it?

4. Say a claim is filed that represents yet another in a series of claims against your client, a hospital, for a patient's contraction of a life-threatening infection during hospitalization. Is the duty to the public outweighed by your duty to the client? Do you even have a duty to the public? Does it matter if this plaintiff's infection has been made worse by the fact that she also has HIV and, therefore, wants confidentiality?

5. Imagine your client is the manufacturer of a medical device that seems to fail with regularity, the manufacturer of a prescription drug that apparently has life-threatening side effects, or is an automobile manufacturer who manufactures an automobile with a gas tank likely to explode in a certain kind of collision. Can you seek confidentiality in the event of settlement? Should you? [3]

6. Finally, suppose your client is a public agency and has just settled a sex discrimination lawsuit. Can you enforce a confidentiality agreement?

Hypothetical scenarios of this type could go on and on (and may have seemed to here). The moral or ethical questions presented are frequently no easier than the legal ones. For the purposes of this article, we will disregard the moral questions and leave them to a higher authority.

At the outset we suggested that if you want confidentiality, you should keep your settlement agreement private and not involve the court. But you may want to consider, and discuss with your client, the fact that if the confidentiality agreement has no teeth, it will have no bite. While plaintiff and his or her counsel may agree to keep their collective mouths shut, what happens if they do not? Does your client get its money back? Such a return of funds is unlikely even with a clause that forfeits some or all the settlement funds. Does a liquidated damages provision offer much benefit? Perhaps some, but it is probable that the liquidated damages provision will be enforced only to the extent that the client can show actual damages. Proof of any such damage is frequently a heavy burden and one unlikely to be met in most instances.

So, does the potential of court disclosure of some, or all, of the settlement terms outweigh the benefit provided by the "bite" of a potential contempt of court threat facing the lawyer or client if one of them discloses the agreement? This is an important question and the answer is, "it depends." Court approval may carry the day if your case will not attract media attention and there is no likelihood of an effort to unseal the agreement based on the "public's (read media's) right to know."

If, on the other hand, it is likely an effort to unseal will be made because the case involves a supposed public health hazard or is otherwise of "public interest," then, assuming that you and your client have no qualms about it, you will not want to depend on the court to keep your secret. According to at least one federal court of

[3] Product liability cases in particular are often cited in support of state Sunshine Acts. Take Florida for example, citing the "growing concern relating to the practice of settling cases, especially in the products liability area, where as part of the settlement the parties will agree not to disclosure information regarding hazardous products, or the court will enter a protective order precluding such disclosure." *See* H.R. Comm. on Judiciary, SB 728, Final Analysis & Economic Impact Statement 2 (Fla. 1990).

appeals, a confidential settlement agreement that the parties deposit under seal with the court is a judicial record that the public is entitled to see. *See Jessup v. Luther*, 277 F.3d 926, 929-30 (7th Cir. 2002). This remains true even if the judge's approval of the agreement was not required and had no legal significance. *Id.* at 929. According to the Seventh Circuit, the public has a right to know the terms of any settlement that a judge agrees to. *Id.* at 930.

A further level of consideration as to whether filing or not filing is preferable is the fact that even when filed with the court, the court can only do so much to protect your client and deter disclosure. Once disclosed and disseminated, the court's authority in stopping further dissemination or recovering disclosed information can only practically extend so far, and the "bite" provided by filing with the court becomes less powerful.

Take, for example, pharmaceutical company Eli Lilly. The company was involved in multi-district litigation concerning its prescription medicine Zyprexa®. *See In re Zyprexa Prods. Liab. Litig.*, MDL No. 1596 (E.D.N.Y.). In an effort to facilitate discovery and protect confidential information, the court entered a protective order which bound all parties, counsel, and consultants from disclosing or producing documents and information marked confidential. *See* Case Management Order No. 3. It also provided that, if necessary, documents that had to be filed with the court could be done so under seal. *Id.* Disclosure or production of confidential information would subject the disclosing individual to sanctions, including contempt of court. *Id.* Suffice it to say that confidential documents were produced, in response to a subpoena, to an attorney pursing unrelated litigation centered on antidepressant medication.[4] This attorney then took the liberty of providing the documents to, among others, *The New York Times* and various web servers that happily printed and/or posted the documents for public viewing.

Alarmed, and rightly so, Eli Lilly sought and obtained an order enjoining further dissemination of the documents and also requiring the return of the documents from the various recipients. While, in theory, the order netted the result Eli Lilly sought, it also lacked any practical effect as the documents, not surprisingly with the assistance of the internet, had already found their way to places as far-reaching as a server in Australia. Of course the documents initially produced could be recouped, and the offending attorney could seek to obtain the copies sent to his chosen round of recipients, but did the court's authority practically extend to those in other countries? These individuals certainly could not be subject to the court's contempt power for allegedly breaching a protective order to which they were neither a party nor had knowledge of. As such, would there be any practical effect to entering an order telling them to remove the confidential material from their websites?

The purpose of discussing the Eli Lilly case is merely to point out that even when a confidential settlement is given teeth by filing it with the court, the court's power to enforce that confidentially and to punish potential disclosers can only go so far. Once information has been disclosed and spread, the court can only do so much to try and unring the proverbial bell.

In light of these considerations, how should one proceed in the scenarios presented? As to the moral questions alluded to above, we will not attempt to provide answers to them, but merely say that some of you will take the position that your master is your client and it is to your master to whom you owe your only duty (aside from our known obligations to the court). Others will have the view that there is a higher duty (and that may be to the public) that requires you to decline participation in any act that will ultimately

[4] For a discussion of this case see Tom Zeller Jr., Documents Borne by Winds of Free Speech, 156 N.Y. Times C3 (Jan.15, 2007).

lead to harm. We do not suggest here that either view is right or wrong. A discussion of the legal, practical, and ethical questions is, however, in order.

Consider Scenario 1. First, claims against the Catholic Church seem to have caught the eye of the media and the public such that a settlement agreement reached and filed under seal with the court related to such a claim will likely attract attention and curiosity. Undoubtedly efforts will be made to discover such settlement agreements. The settlement agreement should, in most instances, be private, and a simple dismissal of the lawsuit will ensue. In an effort to give the settlement some teeth, however, you should consider a provision that should any of the settlement terms become public, then the entire agreement will be made available for inspection by anyone who cares to examine it. It is not unusual for lawsuits of this nature to be brought using only the initials of the plaintiff because of the plaintiff's desire for privacy. Thus, a provision providing for free access by the public to the agreement in the face of disclosure will serve as some incentive to plaintiff to maintain confidentiality as otherwise his/her name becomes public—a circumstance most do not want.

As to confidentiality and the potential exposure of others to harm, that is a circumstance you must discuss with your client as well as the possible future liability (including in some instances punitive damages) presented if confidentiality is maintained. This is also true with respect to the facts set forth in Scenario 2 with the school district. Specifically, knowledge of an employee's propensity to engage in sexual abuse of congregants or students could result in punitive liability should the employee retain his or her position and then a similar claim is made at a later date.[5] Thus, if you believe the allegations, then you should discuss this type of future liability with your client. There is also a very real possibility that the desire for confidentiality may well be outweighed by consideration of future exposure because of injury to others.[6]

In addition to these considerations, a lawyer should also recognize any potential obligations to disclose what would otherwise be considered confidential information. While not requiring disclosure, the ABA Model Rules of Professional Conduct provide that confidential information may be disclosed if a lawyer reasonably believes that disclosure is necessary to "prevent reasonably certain death or substantial bodily harm." Mod. R. Prof. Conduct 1.6(b)(1). The question then becomes whether sex abuse falls under the definition of "substantial bodily harm." Further, with respect to Scenarios 1 and 2, a lawyer would do well to consider any mandatory child abuse reporting requirements imposed by his or her jurisdiction. For example, Oregon law requires that any public or private official, attorneys included, report suspected abuse

[5] In addition to punitive liability school districts in particular could be subject to liability under 42 U.S.C. § 1983 and Title IX of the Education Amendments of 1972, 20 U.S.C. § 1681 *et* seq. *See* Shrum ex. rel Kelly v. Kluck, 249 F.3d 773 (8th Cir. 2001). In Shrum, plaintiff brought claims under § 1983 and Title IX after her son was molested by a teacher who had been previously employed by the defendant superintendent and school district. Following an investigation into a sexual assault complaint against Kluck, the defendant school district and Kluck entered into a confidential settlement agreement that provided, in part, that Kluck would voluntarily resign and the defendant school district would provide him with a positive letter of recommendation. Kluck was later hired at plaintiff's son's school in part because of the recommendation letter from the defendant school district. The court ultimately granted summary judgment to the defendant district as to both claims, but cases such as this should act to provide some notice that under slightly different circumstances, liability could result.

[6] *See* Picton v. Anderson Union High Sch. Dist., 57 Cal. Rptr. 2d 829, 833 (Cal. App. 1996) (A confidential settlement agreement between a school district and a teacher accused of rape and sexual misconduct was ruled in violation of public policy because the school district had a duty to report the allegations to the State Commission on Teacher Credentialing).

or a suspected abuser. *See* Or. Rev. Stat. § 419B.010. Of course there is no shortage of discussion on the conflict with the attorney-client privilege that this statute creates; we mention it solely for purposes of awareness and consideration when entering into confidential settlement agreements in these types of cases.

As to Scenario 3, ethical considerations might weigh against an effort to persuade the offending plaintiff's lawyer to stop suing your client. The District of Columbia Bar has issued an opinion stating that a settlement agreement may not compel counsel to keep confidential and not further disclose in promotional materials or on their law firms' websites public information about the case, such as the name of the opponent, the allegations set forth in the complaint on file, or the fact that the case has settled. D.C. Ethics Op. 335 (2006). According to that opinion, conditions of that nature have the purpose and effect of preventing counsel from informing potential clients of their experience and expertise, thereby making it difficult for future clients to identify well-qualified counsel and employ them to bring similar cases. *Id.* Such restrictive agreements diminish the opportunity for the lawyer to represent future clients in similar matters, a violation of Rule 5.6(b) of the Rules of Professional Conduct.[7] *Id.* Similarly, the Oregon Supreme Court has sanctioned a lawyer who entered into an agreement to be employed by the defendant company against whom he had had considerable success. *In re Conduct of Brandt*, 10 P.3d 906 (Or. 2000).

The message seems clear that plaintiff's counsel cannot enter into such an agreement to limit her practice, and it also seems unwise for defense counsel to suggest or pursue such an agreement.

Scenarios 4 and 5 set forth classic examples of cases quick to draw media scrutiny due to the potential public health hazards that they present. If confidentiality is desired in this type of situation, it is advisable to not file the settlement agreement with the court.[8] And given the potential for cases of this nature to involve the production of highly-sensitive internal documents, a lawyer would be wise to consider the woes of Eli Lilly when drafting the settlement agreement. By building in provisions that provide for a sufficient disincentive to breach, an attorney will assist clients in avoiding similar woes. As to the question of whether confidentiality is advisable, much like was recommended with respect to sex abuse cases, a discussion with the client of potential future liability is warranted and perhaps even a discussion proposing corrective action going forward.

As to Scenario 6, in most jurisdictions, a public body is quite limited in what may be withheld from the public.

In conclusion, answering the question of whether to file a confidential settlement agreement with the court, and more generally whether to seek confidentiality in the first place, requires several layers of

[7] Model Rule 5.6 provides that "A lawyer shall not participate in offering or making: (a) a partnership, shareholders, operating, employment, or other similar type of agreement that restricts the right of a lawyer to practice after termination of the relationship, except an agreement concerning benefits upon retirement; or (b) an agreement in which a restriction on the lawyer's right to practice is part of the settlement of a client controversy."

[8] Even unfiled documents could be subject of a suit to disclose. In Estate of Frankl v. Goodyear Tire & Rubber Co., 853 A.2d 880 (N.J. 2004) consumer protection organizations sought the disclosure of documents protected by a court approved umbrella protective order that applied to all materials exchanged during discovery. The organizations claimed that the documents revealed an ongoing safety issue concerning tread separations in a certain model of tire and that the public had a strong interest in seeing the documents because the tires were in such widespread use. The New Jersey Supreme Court issued an opinion stating that "unfiled documents in discovery are not subject to public access." Although reassuring, this is not the first, and undoubtedly will not be the last, time that disclosure of confidential unfiled documents is sought in the name of public safety.

analysis. It is not a simple aim and shoot matter. There are no hard and fast rules that provide easy answers to the request for confidentiality, whether from the client or the adverse party. But, perhaps, we have provided food for thought when considering a confidential settlement agreement.