

**THE PARADOXICAL NATURE OF THE SARBANES-OXLEY
ACT AS IT RELATES TO THE PRACTITIONER REPRESENTING A MULTINATIONAL CORPORATION**

JASON THOMPSON*

I.	INTRODUCTION.....	265
II.	SARBANES-OXLEY ACT.....	266
III.	THE CONFIDENTIALITY CONFLICT: THE SARBANES-OXLEY'S IMPACT ON ATTORNEYS.....	267
IV.	EUROPEAN LAWS: <i>MCDONALD'S</i> AND <i>EXIDE TECHNOLOGIES</i>	271
V.	THE SOLUTION.....	277
VI.	CONCLUSION.....	280

I. INTRODUCTION

Many people are unfamiliar with the Sarbanes-Oxley Act (“SOA”), despite the fact the Act impacts many people within the United States, as well as those purchasing American goods in other countries or working for American companies outside the U.S. The SOA not only has a tremendous impact on the way businesses are run, but also costs businesses significant amounts of money to comply with the many different sections.¹ Many legal practitioners lack an understanding of what the Sarbanes-Oxley Act actually does and how to advise clients on compliance if their company chooses to expand on an international level. If pressed, many likely would respond that the Sarbanes-Oxley Act has something to do with corporate fraud and avoiding scandals, such as Enron and WorldCom, along with all the financial difficulties these events caused their stockholders and U.S. citizens. This article addresses extraterritorial aspects of the Sarbanes-Oxley Act, and

* J.D. University of Oklahoma College of Law; L.L.M. Stetson University College of Law. The author would like to thank Professors Luz Nagle, Mark Bauer, Sally Waters and Amy Thompson, Esq. for their comments and encouragement.

1. Deborah Solomon, *Corporate Governance (A Special Report): At What Price? Critics say the cost of complying with Sarbanes-Oxley is a lot higher than it should be*, WALL ST. J. Oct. 17, 2005, at R3. In fiscal year 2001, the average cost of auditing fees among S&P 500 companies was \$2,934,000, S&P Mid-Cap 400 was \$716,000, and S&P Small-Cap 600 was \$362,000. In 2002, the year Sarbanes-Oxley became law, the cost was \$4,048,000 for S&P 500 companies, \$951,000 for S&P Mid-Cap 400, and \$485,000 for S&P Small-Cap 600. In 2003, the amount increased to \$4,809,000 for S&P 500 companies, \$1,135,000 for S&P Mid-Cap 400, and \$567,000 for S&P Small-Cap 600. In 2004, the average amount was \$7,443,000 for S&P 500 companies, \$2,177,000 for S&P Mid-Cap 400, and \$1,042,000 for S&P Small-Cap 600. *Id.*

explores generally the many conflicts that arise when companies must comply with the Act.

II. SARBANES-OXLEY ACT

In response to corporate scandals of the late 1990s and early 2000s,² Congress enacted the SOA.³ The SOA is perhaps the most sweeping set of laws relating to public companies since the passage of the depression-era laws.⁴ The SOA passed almost unanimously through both the House of Representatives⁵ and the Senate.⁶ At the time of passage, it was, and remains, the largest piece of legislation to pass through Congress since the Patriot Act. At the time of signing, President George W. Bush said: "My administration pressed for greater corporate integrity. A united Congress has written it into law. [T]oday I sign the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt. This new law sends very clear messages that all concerned must heed."⁷ The President went on to say, "[w]ith this law [SOA], we have new tools . . . and we will use those tools aggressively to defend our free enterprise system against corruption and crime."⁸

The SOA is a colossal piece of legislation in both size and scope. It created the Public Company Accounting Oversight Board, an independent board that regulates and provides supplementary oversight of the Securities and Exchange Commission ("SEC"), which is responsible for regulating certified public accountants practicing before it.⁹ The SOA also limits simultaneous audit and non-audit services that a public accounting firm can perform for

2. Brian Kim, *Recent Development: Sarbanes-Oxley Act*, 40 HARV. J. ON LEGIS. 235, 236 (2003). In December of 2001, Enron filed the largest bankruptcy in U.S. history and as a result 20,000 employees of Enron lost a total of \$1,200,000,000 in 401(k) plans as the stock fell from \$90 per share to pennies. Enron executives sold \$994,000,000 in shares of Enron stock from January of 1999 to May 2002. *Id.*

3. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 1702, 116 Stat. 745 (codified as amended at 15 U.S.C. §§ 78j-o, 7201(2002)).

4. EDWARD F. GREENE, LESLIE N. SILVERMAN, DAVID M. BECKER, EDWARD J. ROSEN, JANET L. FISHER, DANIEL A. BRAVERMAN & SEBASTIAN R. SPERBER, *THE SARBANES OXLEY ACT: ANALYSIS AND PRACTICE 1* (Aspen 2003).

5. *See id.* at 1 (citing 148 CONG. REC. H5480 (daily ed. July 25, 2002) (House of Representatives approving bill by vote of 423-33)).

6. *See id.* (citing 148 CONG. REC. 57365 (daily ed. July 25, 2002) (Senate approving bill by vote of 99-0)).

7. President George W. Bush, Remarks by the President at Signing of H.R. 3763 (2002 WL 1751366) (July 30, 2002).

8. *Id.* at 4.

9. HAROLD S. BLOOMENTHAL, *SARBANES-OXLEY ACT IN PERSPECTIVE* § 1:10 (Audrey M. Simon et al. eds., Thomson West 2004).

the same client.¹⁰ This process is aimed at avoiding situations similar to the Arthur Andersen scandal, of early 2000.¹¹ This means a firm cannot both perform accounting work and auditing for a company.¹²

The SOA also contains a certification requirement focused on improving the quality and reliability of reports filed with the SEC.¹³ One goal of the SOA is to ensure that corporate disclosures are enhanced with more information and reporting done in real time.¹⁴ The SOA mandates that accounting firms producing reports cannot have a conflict with the company that is the subject of the report (as was the case for the accounting firm representing Arthur Andersen).¹⁵ Thus, the current SOA requires more reporting than ever, with increased reliability. Additionally, it requires more people to get involved with the preparation of reports and conduct the necessary audits.¹⁶

III. THE CONFIDENTIALITY CONFLICT: THE SARBANES-OXLEY'S IMPACT ON ATTORNEYS

Although the main focus of Congress' wrath in passing the SOA was chief executive officers (CEOs), chief financial officers (CFOs), and accountants, attorneys did not entirely escape the SOA's expansive reach as evidenced by section 307.¹⁷ Section 307 sets minimum requirements of professional conduct for lawyers, and proscribes that anyone who fails to comply will be disqualified from practicing before the SEC.¹⁸ Additionally, this section requires "an attorney representing an issuer to report evidence of a material violation of securities laws, a breach of fiduciary duty, or similar violations by the company or any agent of the company" to the chief legal officer (CLO) or CEO of the company.¹⁹ If this does not result in appropriate corrective measures, the attorney must then go "up-the-ladder to the audit committee, or a committee of the board consisting of non-management directors, or to the board of directors."²⁰ The SEC, in establishing this rule stopped short of

10. *Id.*

11. In 2000, Arthur Andersen earned \$27 million in consulting fees and \$25 million in accounting fees from Enron. See Kim, *supra* note 2, at 244.

12. *Id.*

13. See BLOOMENTHAL, *supra* note 9, at § 1:10.

14. *Id.*

15. *Id.*

16. *Id.* § 1:13.

17. *Id.* § 1:17.

18. *Id.*

19. *Id.*

20. *Id.*

requiring an attorney to disclose information to the SEC; however, an attorney may choose to disclose confidential information to the SEC in certain cases.²¹ One such case, allows an attorney to use contemporaneous records or reports in defending himself or herself in an investigation for violations of the SOA.²²

The problem with this requirement is that it conflicts with the American Bar Association's (ABA) Model Rules of Professional Conduct, which shape most state rules of professional conduct.²³ The ABA's Model Rules of Professional Conduct state that a lawyer shall not release any information relating to the representation of the client without first gaining the client's permission, which requires consultation and full- disclosure.²⁴ Exceptions to this rule allow an attorney to violate client confidence "to the extent the lawyer reasonably believes it is necessary to prevent the client from committing a criminal act that the lawyer believes is likely to result in *imminent death or substantial bodily harm*."²⁵ The attorney may also use client confidential information in defending or prosecuting an action against the client.²⁶ Further, an attorney may use client confidential information in the defense of a criminal claim or civil suit against the lawyer, based on the conduct involving the client, or in response to allegations pertaining to the attorney's representation of the client.²⁷

The ABA's Model Rules of Professional Conduct clearly conflict with the provisions of the SOA. The SOA disclosure likely will not fall under the exception allowing for disclosure in the case of death or substantial bodily harm. Although disclosure to the SEC is permissive, disclosure to the CEO and auditor is not. If such a disclosure is not made in accordance with the rules of professional conduct established by the ABA and most states, attorneys will be in direct violation of the SOA. If it is made, attorneys will be in violation of the rules of professional conduct. Both the SOA, and most rules of professional conduct, allow for potential disbarment for violating the rule. Based on the SOA provisions for keeping auditors separate and independent, how is this not a contradiction? The most obvious answer is that it is, and will remain a contradiction.

21. *Id.* § 4:25.

22. *Id.*

23. MODEL RULES OF PROF'L CONDUCT (2004), available at http://www.abanet.org/cpr/mrpc/mrpc_toc.html. The practitioner should consult his or her own state rules of professional conduct to determine whether a conflict exists.

24. *Id.* at R. 1.6 (2004), available at http://www.abanet.org/cpr/mrpc/rule_1_6.html.

25. *Id.* (emphasis added).

26. *Id.*

27. *Id.*

The best course for an attorney to follow is compliance with the SOA, as he or she may later use such compliance as a defense in the event that a complaint is brought in front of the regulatory board for the state where the attorney practices. However, the complying attorney must do so with the realization that he or she is violating the ethics rules he or she took a vow to uphold. On the other hand, potential penalties for violating the SOA are quite severe. If any provision of the Securities and Exchange Act, or rule or regulation adopted there under, is willfully violated, the maximum prison sentence is 20 years, with a maximum fine of \$5 million for a natural person,²⁸ or \$25 million for a violator other than a natural person, which includes businesses that must comply with the SOA.²⁹

The primary purpose of the SOA is to prevent the type of corruption and crime that marked the downfall of companies such as Enron, WorldCom, and Arthur Andersen.³⁰ As a means to that end, the U.S. government must obtain information about companies doing business in the U.S. and abroad, as it is not practical for the SEC to investigate all companies within its jurisdiction to determine if proper practices are being observed.³¹ The far more practical means of accomplishing the goals of the SOA is to get the information from those who work for each individual company. Thus, all companies registered with the SEC are required to file with the SEC and certify that all aspects of the SOA are being followed.³² The issue with this solution is that those who are in the position to perpetrate fraud are the same people who file the disclosure statements.

To combat this problem, the SOA provides for employees of a company to have the ability to report the illegal deeds of superiors that fall under the SOA without fear of retaliation.³³ The idea is similar to the whistleblower theory, but the SOA gives the employee a greater sense of security that retaliation against the employee will not occur.³⁴ This is accomplished through anonymous tip-lines where an employee can phone-in information regarding the company they work for, without giving personal information, and without the knowledge of the person about whom the report is

28. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 1106, 116 Stat. 810 (codified as amended at 15 U.S.C. §§ 78j-o, 7201(2002)).

29. *Id.*

30. See Robert G. Vaughn, *America's First Comprehensive Statute Protecting Corporate Whistleblowers*, 57 ADMIN. L. REV. 1, 68 (2005).

31. *Id.*

32. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 1106, 116 Stat. 810 (codified as amended at 15 U.S.C. §§ 78j-o, 7201(2002)).

33. *Id.*

34. Vaughn, *supra* note 30, at 68.

being made.³⁵ Moreover, information provided over a tip-line will not force the reporter to appearing as a witness to testify at a later date.³⁶ This anonymous whistleblower provision of the SOA applies to all companies that are required to file with the SEC pursuant to the terms of the Securities and Exchange Act of 1934, including "companies with any security registered under the Securities Exchange Act of 1934 or any company required to file any reports under that Act."³⁷

Based on the breadth of the SOA and its extraterritorial application, the SOA is one of the most important whistleblower acts.³⁸ Due to the broad reaching definitions of the SOA, certain companies that are either chartered in, or do business in another country, are also required to comply with the SOA's whistleblower provision.³⁹ This is where the inherent problem occurs with this section of the SOA due to its direct conflict with the laws of the European Union.

Generally speaking, courts are hesitant to enforce laws extraterritorially without a direct statement of intent. In the case of the SOA's whistleblower provision, this intent is specifically expressed through five particular aspects of the provision.⁴⁰ First, the provision explicitly applies to foreign entities and foreign companies.⁴¹ Second, the term "employee" is not limited to company employees located within the U.S. or to U.S. citizen employees, employed by companies within the U.S.⁴² Third, disclosures are based on the standards of U.S. law, thus protecting only those disclosures made to regulatory agencies of the U.S. (such as the SEC), members of Congress, and members of congressional committees.⁴³ Fourth, the provision overtly creates a cause of action resulting from its violation, and directs the enforcement to the United States Department of Labor and the courts of the U.S.⁴⁴ Fifth, the law concentrates on the protection of the securities markets of the U.S.⁴⁵ As a result of the whistleblower provision of the SOA, a citizen of a foreign country can be subject to the jurisdiction of the U.S. simply because he or she happens to be employed by a company that is a subsidiary of

35. *See id.*

36. *Id.*

37. Securities Exchange Act of 1934, 48 Stat. 881, 15 U.S.C. §§ 78a-78kk; Vaughn, *supra* note 300, at 68.

38. *Id.*

39. *Id.*

40. *See id.* at 69.

41. *Id.* at 69-70.

42. *Id.* at 70.

43. *Id.*

44. *Id.*

45. *Id.*

a U.S. company or, more broadly, because a company that is chartered in, and does business in, a foreign country chooses to register with, and have securities in the U.S. as a means of raising capital.⁴⁶

The real issue arises when companies fall under the reach of the whistleblower provision of the SOA, as well as the laws of another jurisdiction because of its presence within that country. The companies in this circumstance must comply with the laws of each jurisdiction, even when a specific conflict arises between the laws.⁴⁷ This is impossible for both domestic and foreign companies. The result is that companies failing to comply with the laws of every jurisdiction, in which it is present, are being sued for failure to comply, as evidenced by the recent *McDonald's* and *Exide Technologies* cases.⁴⁸

IV. EUROPEAN LAWS: *MCDONALD'S* AND *EXIDE TECHNOLOGIES*

In addition to the inherent difficulties of complying with the SOA in terms of necessary disclosures, and reports, as well as efforts to avoid corruption and fraud, attorneys and companies also have a litany of other issues to confront when companies choose to go multinational. Provisions of the SOA, such as the anonymous tip-line, conflict with laws in other jurisdictions such as the European Union. One of these conflicts arose with the European Union's enactment of a law dealing with the transfer of personal information to a third country.⁴⁹ The law states that the "data subject" should have access rights to all the information relating to him and have the right to erase or block the data.⁵⁰ This right causes major problems for a system operating off an anonymous tip-line. The law further mandates that in transfers of data to a third country, the "data subject" should have the proper information to object or withhold consent for the transfer of the data.⁵¹

46. *See id.*

47. *Id.*

48. *Exide Technologies*, CNIL (La Commission Nationale de L'Information et des Libertés) (The French Protection Authority) Decision 2005-111 (May 26, 2005), available at <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1246367122005> (English translation); *McDonald's France*, CNIL (La Commission Nationale de L'Information et des Libertés) (The French Protection Authority) Decision 2005-110 (May 26, 2005), available at <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1243487122005> (English translation).

49. Commission Decision 2001/498, 2001 O.J. (L 181) 19 (EC).

50. *Id.* §13.

51. *Id.* §14.

Furthermore, the data exporter and the data importer, are deemed to be jointly and severally liable for any violations.⁵²

McDonald's and Exide Technologies, two American companies doing business in France, have both discovered the problems with being multinational corporations that must comply with the SOA. Both companies have had identical cases in French courts.⁵³ As the facts and analysis of the cases are in essence identical, only the *McDonald's* case will be analyzed in this article.⁵⁴

The *McDonald's* action involved La Commission Nationale de L'Information et des Libertés ("CNIL"), the French Data Protection Authority, and McDonald's failure to comply with the CNIL.⁵⁵ McDonald's made a request of the CNIL for authorization to put into place a system of "professional integrity."⁵⁶ Under the requested system, found in international McDonald's Group's "Code of Ethics," the staff of the French subsidiaries would be allowed to report to the American parent company about the behavior of co-workers and that of their colleagues.⁵⁷ This action was "deemed contrary to the French legal rules, as well as the Code of Ethics."⁵⁸ The procedures proposed by McDonald's would not affect all of the employees of McDonald's in France.⁵⁹ McDonald's project would only apply to head office employees, managers, and executives of the one hundred seventy-five restaurants amounting to approximately one thousand people.⁶⁰ The contents of the reports sent to the parent company in the U.S. would be recorded in a central file under the direction of the Director of Ethics for McDonald's.⁶¹ Each report would receive a report number so as to ensure the confidentiality of the report and the anonymity of the informant.⁶² Once the Director of Ethics received the report, he or she would communicate its contents to general counsel for McDonald's

52. *Id.* § 18.

53. Exide Technologies, CNIL (La Commission Nationale de L'Information et des Libertés) (The French Protection Authority) Decision 2005-111 (May 26, 2005), available at <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1246367122005> (English translation); McDonald's France, CNIL (La Commission Nationale de L'Information et des Libertés) (The French Protection Authority) Decision 2005-110 (May 26, 2005), available at <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1243487122005> (English translation).

54. *Id.*

55. McDonald's France, CNIL (La Commission Nationale de L'Information et des Libertés) (The French Protection Authority) Decision 2005-110 (May 26, 2005), available at http://www.faegre.com/articles/downform2.asp?doc_num=2&aid=1691 (English translation).

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

France.⁶³ General Counsel would then forward the information to the appropriate service manager depending on the nature of the alleged offense.⁶⁴ The department director would then decide whether or not to open an investigation, and if so decided, the director would send the information only to those persons involved in the investigation.⁶⁵ The department director would inform the general counsel (in France) of the investigation and coordinate with him or her regarding the investigation.⁶⁶ If the investigation is of a member of management of McDonald's France, the investigation would be dealt with by the American parent company.⁶⁷

The French court analyzed the provisions of McDonald's plan under the provisions of several relevant laws.⁶⁸ First, the court analyzed McDonald's plan in light of the January 6, 1978 law (Article 3).⁶⁹ This law is used by the court to determine whether jurisdiction was proper over McDonald's plan.⁷⁰ The court relied heavily on the encouragement of McDonald's France to use the system and the steps taken by the company to ensure the anonymity of the person who makes reports about colleagues.⁷¹ The court thus, determined that jurisdiction was proper to review McDonald's plan, but found that McDonald's plan did not comply with French law.⁷² In so finding, the court held:

63. *Id.*

64. *Id.* (including the Human Resources Director, Security Director, and Financial and Accounting Director).

65. *Id.*

66. *Id.*

67. *Id.*

68. McDonald's France, CNIL (La Commission Nationale de L'Information et des Libertés) (The French Protection Authority) Decision 2005-110 (May 26, 2005), *available at* <http://www.theworldlawgroup.com/newsletter/details.asp?ID=1243487122005> (English translation).

69. *Id.* (the law is unnamed, only represented by date).

70. *Id.*

71. *Id.*

72. The law dated January 6, 1978 is also known as the "Data Protection Act," *available at* http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83516#_ftnref3.

The Data Protection Act was enacted in 1978 and covers personal information held by government agencies and private entities. This act provides that anyone wishing to process personal data must register and obtain permission in many cases relating to processing by public bodies and for medical research. Individuals must be informed of the reasons for collection of information and may object to its processing either before or after it is collected. Individuals have rights to access information being kept about them and to demand the correction and, in some cases, the deletion of this data. Fines and imprisonment can be imposed for violations.

Id.

implementation by an employer of a system designed to gather personal data from employees, in any form whatsoever, concerning behavior contrary to company rules or contrary to the laws attributable to their colleagues, which could lead to an organized system of professional denunciation, can only give rise to a reservation in regard to the Law dated January 6, 1978 as amended and notably Article 1 of such law.⁷³

The French court also held that the possibility of establishing the tip-line in an anonymous manner “could only re-enforce the risk of slanderous denunciations.”⁷⁴ Based on the application of French law, the court denied McDonald’s request for permission to implement the plan of the tip-line.⁷⁵

Similar to the difficulties encountered by McDonald’s and Exide Technologies in France, Wal-Mart attempted to implement a similar anonymous tip-line in Germany.⁷⁶ A labor group in Germany sued Wal-Mart of Germany based on Wal-Mart’s implementation of an anonymous hotline.⁷⁷ The case went before the Wuppertal Labour Court on oral argument on June 15, 2005.⁷⁸ The German court reached the same decision that the anonymous tip-line instituted by Wal-Mart, much like that of McDonald’s and Exide, was in violation of local law; however, the German court based the decision on a different rationale.⁷⁹ The case was brought by the Central Works Council in Germany, established in the area

73. McDonald’s France, CNIL (La Commission Nationale de L’Information et des Libertés) (The French Protection Authority) Decision 2005-110 (May 26, 2005), available at http://www.faegre.com/articles/downform2.asp?doc_num=2&aid=1691 (English translation).

74. *Id.*

75. *Id.*

76. Mark E. Schreiber et al., *Anonymous Sarbanes-Oxley Hotlines in the E.U.: Practical Compliance Guidance for Global Companies*, BNA INTERNATIONAL WORLD DATA PROTECTION REPORT, at 3 (Aug. 2005).

77. Wuppertal Labour Court, 5th Division, 5 BV 20/05, June 15, 2005 (F.R.G.).

78. This case is not listed in any of the official American case law databases. A limited translation is available at <http://cms-hs.com>. The author of this work received a translation of the case courtesy of Christian Runte of CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern Registerangaben located in Muenchen, Germany (English translation on file with author).

79. Global Compliance Services, *Update Regarding Compliance with Sarbanes-Oxley in Europe*, available at <http://www.globalcompliance.com/pdf/sarbox-alert3.pdf> (last visited Oct. 28, 2005). Wal-Mart appealed the decision and oral argument on the appeal was set for November 14, 2005. The appellate court stated that an opinion on the appeal should be released approximately three weeks after the argument. *Id.*

of work that Wal-Mart is engaged within Germany.⁸⁰ The defendant in this action was classified by the court as a German subsidiary of the U.S. firm of Wal-Mart, Inc.⁸¹

In this case, Wal-Mart operated a telephone hotline.⁸² The employees of Wal-Mart in Germany were encouraged to utilize the telephone hotline for anonymous reporting of violations of the internal code of conduct at Wal-Mart by both co-workers and members of management.⁸³ Wal-Mart issued a “quick guide” of the code of conduct that Wal-Mart distributed to its employees.⁸⁴ The quick guide stated in relevant part: “Should you have any questions or want to report a possible violation of the code of conduct: 1. Please make use of the open door policy and/or 2. Please call the code of conduct telephone hotline.”⁸⁵ The store managers were given posters regarding Wal-Mart’s code of conduct that were to be permanently displayed at every Wal-Mart human resources department.⁸⁶ In the action, the German group requested that Wal-Mart stop using the ethics guide of the code of conduct and from the operation of the ethics hotline.⁸⁷ The German group argued that publishing the code of conduct, and compelling the employees to take note of the code, forced employees to abide by the terms of the code.⁸⁸ Wal-Mart contended that the hotline was voluntary and that employees were not forced to use the line.⁸⁹ Wal-Mart also contended that the implementation of the hotline was “a permissible concretization of the employee’s ancillary duty to prevent harm.”⁹⁰

The court held that the tip-line and displaying of the poster were in violation of German law.⁹¹ The Court determined it had jurisdiction under the German Works Constitution Act.⁹² The court held further, that the German Works Constitution Act is applicable to all businesses in Germany whether or not they originated as German or international businesses.⁹³ In determining

80. Wuppertal Labour Court, 5th Division, 5 BV 20/05, June 15, 2005 (F.R.G.) at I. Wal-Mart is a commercial business that operates 74 branches in Germany and employs approximately 10,500 employees. *Id.*

81. *Id.*

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

91. *Id.* at II.

92. *Id.*

93. *Id.*

jurisdiction, the court also held that when a company introduces a standard of conduct the employee representative in each affected country may exercise the rights provided in that country.⁹⁴ The court determined that the provision of rights in the German Works Constitution Act are mandatory and cannot be affected by instructions from the foreign parent company.⁹⁵ The court reasoned that encouraging employees to report unethical conduct, or violations of an internal code of conduct by means of an anonymous tip-line violates section 87(1) of the German Works Constitution Act.⁹⁶ The court reasoned that even though the provisions of Wal-Mart's code of conduct do not require employees to utilize the tip-line, it still provides for a means of reporting misconduct and further, it is tantamount to the order of conduct within the company. The court also reasoned that a certain provision of the code of conduct states that failure to comply with the code of conduct will result in disciplinary action and possibly termination.⁹⁷ Thus, employees of Wal-Mart are effectively obligated to act a certain way within the company.⁹⁸

The court determined that the installation of the hotline was done with the intent to monitor employee conduct.⁹⁹ The fact that the hotline would be operated anonymously was irrelevant.¹⁰⁰ The court took issue with the fact that under the current state of technology, tip-line caller identities could be determined.¹⁰¹ The court determined that in order for Wal-Mart to avoid a €250,000 fine for each case of violation, Wal-Mart must stop from advising employee compliance with the ethics directives in the code of conduct and stop placing posters in locations throughout Germany.¹⁰² The German court also determined that in order for Wal-Mart to avoid a fine of €250,000 for each case of violation, they must stop operating the telephone hotline.¹⁰³

It is interesting to note that although the courts of France and Germany resulted in a decision against an anonymous hotline to allow employees of subsidiaries of American companies to report unethical behavior, the French court based its decision on the right

94. *Id.*

95. *Id.*

96. *Id.* The German Works Constitution Act (Betriebsverfassungsgesetz) states: "the works council shall have the right of co-determination . . . in matters relating to the rules of operation of the establishment and the conduct of employees in the establishment." *Id.*

97. *Id.*

98. *Id.*

99. *Id.* §5.

100. *Id.*

101. *Id.*

102. *Id.* at I.

103. *Id.*

of the person about whom the report is made to know the contents of such a report.¹⁰⁴ The French court relied heavily on the potential of the falsity of accusations when anonymity is allowed for the accuser.¹⁰⁵ The German court, on the other hand, worried that the person who made the accusation might have his or her identity revealed through technology even though the hotline is intended to be anonymous.¹⁰⁶ No matter what the reason, the problem is still the same for American companies. How can a company comply with the SOA while avoiding hefty fines from E.U. countries?

V. THE SOLUTION

In response to the *McDonald's* and *Excide Technology* cases, CNIL issued a statement on September 28, 2005, stating it is preparing to issue recommendations regarding SOA compliance, along with compliance with French data protection laws.¹⁰⁷ The statement reiterates that the CNIL refuses to authorize projects that involve the use of hotlines that will presumably be used to encourage or allow workers to report the inappropriate behavior of co-workers.¹⁰⁸ The CNIL acknowledged the difficulty of compliance with the SOA and the data protection laws of France. As such, CNIL sent a letter to the SEC on June 29, 2005, and again on July 29, 2005, regarding conflicts in the two sets of laws.¹⁰⁹ In the letter, the CNIL asked whether the SEC plans to use its capabilities to sanction U.S. companies that do business in France that are not in full compliance with the SOA.¹¹⁰ The French requested that the SEC grant an additional three months beyond August 31, 2005 in order to attempt to reach an agreement whereby companies can comply with both U.S. and French (European Union) laws.¹¹¹ The SEC responded on August 10, 2005, and indicated a willingness to be flexible and work with the CNIL to reach a conclusion that is acceptable to both countries.¹¹²

The CNIL drafted guidelines and invited comments in an attempt to fix the matter in France and deal with the conflict of law

104. *Id.*

105. *Id.*

106. *Id.*

107. See *Lignes Éthiques, Whistleblowing: La CNIL Prepare des Recommandations à l'Usage des Entreprises*, <http://www.cnil.fr/index.php?id=1870> (English translation on file with author).

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.*

issue.¹¹³ The guidelines of the CNIL appear as though they will deal at least with some of the difficulties of the SOA and data protection laws, but they by no means fix all the problems.¹¹⁴ The guidelines do show progress as they are the result of a collaboration of the CNIL, attorneys and firms working in the multinational arena.¹¹⁵

Although it appears as though the issue may be settled in France, it still remains for the other 24 countries of the E.U. Within the 25 countries of the E.U., each country has the ability to enforce and interpret the E.U.'s data protection laws as each country sees fit.¹¹⁶ This may lead to 25 different interpretations of the tip-line provision of the SOA.¹¹⁷ For example, the United Kingdom Information Commissioner's Office does not find error in the SOA hotlines.¹¹⁸ If the companies properly investigate the hotline claims, inform the accused, and provide the accused due-process rights, the U.K. apparently will continue to not have an issue with the hotlines.¹¹⁹ However, the U.K. does caution that British law might be violated if a company was to take the anonymous tip without question and act without conducting an impartial investigation.¹²⁰

113. See Robert Bond & Greg Campbell, *Sarbanes Oxley Ethical Hotlines: CNIL Publish Draft Guidelines*, Nov. 7, 2005, http://www.faegre.com/article_1729.aspx; see also <http://www.cnil.fr>.

114. See Global Compliance Services, *Sarbanes Oxley Compliance*, Oct. 28, 2005, <http://www.globalcompliance.com/pdf/sarbox-alert3.pdf>. It is likely that the guidelines adopted by the CNIL will serve as a model for other E.U. member states. The CNIL stated that whistleblower hotlines such as those contemplated by the SOA are not generally forbidden under French law. However, given that personal information is being collected through the hotlines, there must be adherence to the French Data Protection Laws. This mandatory compliance means that information must be collected fairly, those having their information collected must be informed, and have the ability to object to the collection for "legitimate reasons," as well as the right to remove incorrect information. In the guidelines, the CNIL recognized that SOA requires anonymous tip-lines and thus, did not prohibit anonymous reporting. The CNIL did require that hotline operators give the option to those reporting whether to provide their name. Further, the CNIL requires operators to inform reporters that reporting is not required. Companies operating tip-lines are prohibited from publicizing or encouraging anonymous reporting. The CNIL rejected general hotlines, but approves those limited to information regarding auditing and accounting issues. The CNIL also wants to limit the type of personnel that have access to tip-lines, allowing access to those involved in financial matters, excluding categories of employees such as factory workers. *Id.*

115. *Id.*

116. David Reilly & Sarah Nassauer, *Tip-Line Bind: Follow the Law in U.S. or E.U.?* WALL ST. J., Sept. 6, 2005, at C1.

117. By definition of the SOA having a stock listed on a U.S. exchange subjects the company to the SOA and thus, the tip-line requirement. See BLOOMENTHAL, *supra* note 9.

118. See Reilly & Nassauer, *supra* note 116. The U.K. is the E.U. country with the most companies listed on the U.S. markets. *Id.*

119. *Id.*

120. *Id.*

The lack of uniformity among E.U. nations and conflict between the SOA and E.U. data protection laws place multinational companies in precarious positions.¹²¹ As a result of the conflicting laws, some European companies are presently seeking to deregister their stocks on U.S. markets.¹²² Doing so would remove the companies from the requirements of the SOA, allowing them to operate without the restrictions imposed by it, and clear them from the tip-line requirement.

Practitioners who represent clients that are either subject to the SOA and conduct business in Europe or are European companies subject to the SOA, are faced with a difficult situation. At present, it appears as though a company cannot comply fully with both the SOA and E.U. laws. So, what is the proper course of action? It appears as though the best course of action is to comply with E.U. laws because the SEC has not shown an inclination to act on the tip-line bind. Certain countries within the E.U. are clearly not opposed to taking action as indicated by the *Excide Technologies*, *McDonald's* and *Wal-Mart* actions.¹²³ Although this seems to be the prudent course of action at present, the SOA and its hefty penalties will hang over the heads of companies and attorneys like the sword of Damocles.¹²⁴

What is the proper solution? If the SEC exempts the portions of companies that do business in Europe from the tip-line provision of the SOA, it will in effect give those wishing to commit fraud a road map — simply move the fraud to the European portion of the company. European countries will also not want to simply exclude those companies that fall under the SOA from compliance with the E.U. data protection laws.

It seems as though the appropriate solution lies in the middle. Those companies that are subject to the SOA merely because of registration with the SEC, but that are located in and do business in Europe, should be excluded from the tip-line provisions of the SOA. By contrast, those companies that are in effect American companies doing business in Europe should be exempt from E.U. data protection laws and allowed to comply fully with the SOA. This will keep companies from deregistering in the U.S. and not discourage American companies from doing business in Europe for fear of non-compliance with the SOA or E.U. laws.

121. *See id.*

122. *Id.*

123. *Id.*

124. *See id.*

VI. CONCLUSION

The Sarbanes-Oxley Act causes difficulty for the practitioner in representing clients who are subject to the Act, as well as laws of other countries. When representing a client that is subject to Sarbanes-Oxley, as well as laws of other countries, it is prudent to determine if compliance with Sarbanes-Oxley will conflict with foreign laws. Also, the practitioner should be concerned with reporting requirements of Sarbanes-Oxley as they relate to the rules of professional conduct of both the American Bar Association and the relevant state jurisdiction of the attorney.

If the practitioner is representing a company that is subject to the SOA and foreign laws, especially a country within the E.U., it is prudent to be aware of the data protection laws within that country.¹²⁵ A company may potentially find itself in a position where it is impossible to comply fully with all laws. Although the SEC has verbally stated it will not pursue those cases, it should make the practitioner uncomfortable to rely on such unofficial verbal statements.

The SOA also raises the issue of disclosure in the event of wrongdoing relative to the SOA. The practitioner should consult the rules of professional conduct in his or her state and compare his or her ethical duty with the SOA reporting requirements. It is also essential for the practitioner to define who he or she represents — the corporation, board of directors, or company management.

125. Or equivalent if not in the E.U.