International Lawyer

Volume 36 | Number 1 Article 7

2002

Diligence Due in the Era of Globalized Terrorism

Joe Kendall

Pamela O. Barron

Mark H. Allenbaugh

Recommended Citation

Joe Kendall et al., *Diligence Due in the Era of Globalized Terrorism*, 36 INT'L L. 49 (2002)
https://scholar.smu.edu/til/vol36/iss1/7

This Symposium is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

The Diligence Due in the Era of Globalized Terrorism

THE HONORABLE JOE KENDALL,* PAMELA O. BARRON,** AND MARK H. ALLENBAUGH***

I. Introduction: The Two Sides of Globalization

We must all hang together, or assuredly we shall all hang separately.

—Benjamin Franklin[1]

[A]fter America was attacked, . . . [w]e were reminded that we are citizens, with obligations to each other, to our country, and to history. We began to think less of the goods we can accumulate, and more about the good we can do.

—President George W. Bush[2]

"Globalization" and "terrorism" are perhaps the most politically charged terms in public discourse today. Generally speaking, globalization and terrorism, respectively, represent the ideologically opposite goals of peaceful cooperation and violent alienation. Globalization refers to "the observation that in recent years a quickly rising share of economic activity in the world seems to be taking place between people who live in different countries (rather than in the same country)."[3] According to the World Bank, "Globalization can be sum-

*Commissioner, United States Sentencing Commission. Partner, Provost Umphrey, Dallas, Texas. Former United States District Judge for the Northern District of Texas (1992–2002). Judge Kendall currently serves as a Commission liason to Congress on terrorism issues.

**Deputy General Counsel, United States Sentencing Commission. Ms. Barron currently serves as Chair of the Commission's Terrorism Team and is past Chair of the Commission's Nuclear, Biological and Chemical Weapons Team. Ms. Barron is a former Special Assistant United States Attorney in the Eastern District of Virginia.

***Associate, Montedonico, Belcuore & Tazzara, P.C., Washington, D.C; Adjunct Professor, George Washington University Department of Philosophy. Prior to entering private practice, Mr. Allenbaugh served as a Staff Attorney in the Office of General Counsel for the United States Sentencing Commission where he was assigned to the Commission's Economic Crimes Policy Team and Terrorism Team.

1. JOHN BARTLETT, FAMILIAR QUOTATIONS 310 (16th ed. 1992) (remark made to John Hancock at the signing of the Declaration of Independence, July 4, 1776).

2. George W. Bush, President of the United States of America, The President's State of the Union Address, Washington, D.C. (Jan. 29, 2002), *available at* http://www.whitehouse.gov/news/releases/2002/01/print/20020129-11.html.

3. THE WORLD BANK GROUP, ASSESSING GLOBALIZATION, *available at* http://www.worldbank.org/economicpolicy/globalization/ag01.html.

marized as the global circulation of goods, services and capital, but also of information, ideas and people."[4]

There are, furthermore, two main facets of globalization:

> The first is technical progress especially in information technology, international communication and global transportation. Not only goods but also services and knowledge can flow much more easily because of innovations such as the Internet. The second major development is the shift in policy orientation as governments everywhere have reduced barriers that had curbed the development of domestic markets and their links to the international economy.[5]

In contrast to the cooperative nature of globalization, terrorism represents "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[6] According to the National Commission on Terrorism, "People turn to terrorism for various reasons. Many terrorists act from political, ideological, or religious convictions. Some are simply criminals for hire. Others become terrorists because of perceived oppression or economic deprivation."[7] In all events, the defining feature of terrorism is its attempt to achieve political ends through violent and unlawful means.[8]

Consequently, the threat terrorism poses to globalization is self-evident. Ironically, but not surprisingly, as globalization opens up world markets and eases communication and transportation, it also makes vulnerable the very infrastructure that makes such trade and communication possible in the first place. Indeed, terrorists to advance their own violent political agendas now are exploiting the very same technological advances and governmental policy orientations that promote globalization. In a sense, then, terrorism is the "dark side" of globalization.[9]

Part I of this article reviews the United States' legislative response to the tragedies of September 11, 2001. Among the many changes made by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001,[10] Title II of the Act provides for enhanced governmental

4. THE WORLD BANK GROUP, POVERTY IN AN AGE OF GLOBALIZATION 1 (Oct. 2000), *available at* http://www.worldbank.org/economicpolicy/globalization/documents/povertyglobalization.pdf.

5. *Id.*

6. 28 C.F.R. § 0.851 (2000).

7. NATIONAL COMMISSION ON TERRORISM, 105TH CONG., REPORT: COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM III (2000), *available at* http://w3.access.gpo.gov/nct/nct1.pdf.

8. *See, e.g.*, 18 U.S.C. § 2332b(g)(5) (2001) (defining a "Federal crime of terrorism" as "an offense that (A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and (B) is a violation of" one of 38 listed predicate offenses ranging from murder of U.S. officials to diseminating computer viruses). Thus, a "Federal crime of terrorism" is a listed offense that also has a political motive. As the motive is not an element of the offense, however, there is no crime of terrorism per se. Rather, the definition of a federal crime of terrorism serves to give the Attorney General of the United States primary investigative authority into such offenses. *See* 18 U.S.C. § 2332b(f). Likewise, the definition serves to identify a sentencing factor—political motive—for which the United States Sentencing Commission was tasked by Congress to provide a sentencing enhancement. *See* UNITED STATES SENTENCING COMMISSION, FEDERAL SENTENCING GUIDELINES § 3A1.4 (Nov. 2001) [hereinafter USSG]; USSG App. C., amends. 526, 539, 565; United States v. Graham, 275 F.3d 490 (6th Cir. 2001) (discussing the applicability of USSG § 3A1.4).

9. *See* Craig Hall, Terrorism's Burdens on Globalization, Speech at Southern Methodist University Dedman School of Law (Feb. 7, 2002); *see also* Mr. Hall's article in this issue, *The Wake-up Call of Terrorism*, at 125.

10. Pub. L. 107–56, 115 Stat. 272 (2001).

surveillance procedures in cases relating to terrorism and eases government access to electronic communications or stored computer data, while Title III of the Act provides for various "enhanced" due diligence requirements to financial institutions to prevent and detect money laundering.

In light of these increased due diligence requirements on the financial front, and the government's concern about the exploitation of electronic media for illicit purposes, Part II of the article discusses compliance programs and the role they play with respect to civil liability and enforcement actions as well as criminal investigations and prosecution, and more directly, the mitigating effect they can have with respect to sentencing should an organization be convicted of an offense. Part III of the article argues that in order to combat terrorism, the diligence now due must be "globalized." For compliance programs to be deemed "effective" in the era of globalized terrorism, increased diligence is due across a variety of fronts: financial, cyber, and personnel.

Finally, as the world fights terrorism on a military front, we conclude that the integrity of our infrastructure can be maintained, and the benefits of globalization can be enjoyed, only if the private sector establishes sufficiently vigilant industry auditing and reporting standards. Governments simply cannot do it alone; the private sector must take the lead in minimizing terrorism's threat to globalization. Recognizing the central role effective compliance programs play in the fight against terrorism is a necessary first step toward achieving this goal.

I. Terrorism Goes Global

On Tuesday, September 11, 2001, four commercial airliners were hijacked from various airports along the eastern seaboard in a coordinated terrorist attack on the United States. Two of the airliners were flown at high speed into each of the 110-story twin towers of the World Trade Center located in New York City, causing the deaths of thousands of American civilians and foreign nationals, including dozens of innocent passengers onboard the airliners. Shortly after the attacks on the "Twin Towers," another airliner was flown at high speed into the Pentagon in Arlington, Virginia, causing the deaths of approximately 200 military and civilian personnel. The remaining airliner crashed into a field approximately seventy miles southeast of Pittsburgh, Pennsylvania.

All told, over 3,000 Americans and foreign nationals lost their lives as a result of these terrorist attacks—more than the number of deaths that resulted from the surprise military attack on Pearl Harbor on December 7, 1941, and over fifteen times the number of deaths that resulted from the Oklahoma City Bombing on April 19, 1995. The terrorist attacks of September 11, 2001, thus constitute the largest loss of civilian life from a criminal act in the history of the United States.[11]

The hijackers widely are believed to be members of, or associated with, al Qaeda (Arabic for "The Base"), an international Islamic fundamentalist terrorist sect operated by Saudi exile Osama bin Laden.[12] The purpose of these terrorist attacks generally is believed to

11. For an exhaustive review of the events that transpired and links to a variety of resources, see *Special Report – America Attacked*, WASH. POST, *available at* http://www.washingtonpost.com/wp-dyn/nation/specials/attacked/.

12. For a brief biography of bin Laden and an overview of the relationship between bin Laden and al Qaeda, see YEHUDIT BARSKY, THE AMERICAN JEWISH COMMITTEE, TERRORISM BRIEFING: OSAMA BIN LADEN AND AL-QA'IDA (Sept. 13, 2001), *available at* http://www.ajc.org/terrorism/BriefingsDetail.asp?did=221&pid=737.

have been "to influence or affect the conduct of government by intimidation or coercion."[13] According to the President, although "[t]he attack took place on American soil, . . . it was an attack on the heart and soul of the civilized world. And the world has come together to fight a new and different war . . . A war against all those who seek to export terror, and a war against those governments that support or shelter them."[14] Consequently, on Wednesday, September 12, 2001, Congress passed a near-unanimous joint resolution expressing, among other things, the House and Senate's support of "the determination of the President . . . to bring to justice and punish the perpetrators of these attacks *as well as their sponsors*."[15]

As the current war on terrorism continues, it has become evident that it cannot be won along the military front alone. Rather, as the investigations into the terrorist attacks have revealed, terrorism must be fought along financial, electronic, and personnel fronts: we must attack not only the perpetrators, but also the sponsors and the means by which terrorists achieve their ignoble ends. Although religious fanaticism and a dogmatic hatred of the United States motivated the events of September 11, money, communication, technology, and a host of witting and unwitting facilitators made the devastation of September 11 possible.

For example, it now is clear that the al Qaeda hijackers used a variety of tools, from credit card fraud to the exploitation of charitable organizations and financial institutions, to obtain and transfer funds through various financial institutions to locales across the globe in order to advance their operations. Similarly, reports have surfaced that the hijackers also exploited the information-rich Internet to research potential targets for attack—including nuclear weapons facilities, as well as to obtain information on constructing explosives. And not only did the Internet provide a treasure-trove of helpful information to them, it also served, and continues to serve, as a superb vehicle for surreptitiously coordinating "sleeper cells" to undertake terrorist attacks through the use of encrypted e-mails, as well as through the little-known method of steganography: the embedding of encrypted messages in the images of otherwise innocuous-looking Web pages.[16]

Given these concerns about the financial, electronic, and personnel fronts in the War on Terrorism, Congress passed sweeping legislation that, in conjunction with the ongoing military campaign, will make it harder for terrorists to exploit for evil ends the same tools that have made globalization possible. We review this legislation below, and, in the section immediately following, we discuss recent and ongoing counterterrorism efforts by the United States Sentencing Commission to deter, and more importantly, prevent acts of terrorism altogether.

A. The Government Response: The USA PATRIOT Act

On October 26, 2001, the President signed into law the USA PATRIOT Act of 2001 (hereinafter "the Act").[17] Among other things, the Act broadened the investigatory power

13. 18 U.S.C. § 2332b(g)(5); President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001).

14. The Coalition Information Centers, The Global War on Terrorism—The First 100 Days 3 (Dec. 20, 2001).

15. S. Res. 22, 107th Cong. (2001) (emphasis added).

16. *See U.S. Officials Fear Islamic Web Site Has Secret Codes*, Nat'l Post, Dec. 10, 2001, at A10; Kevin O'Brien, *Carnivore Feeds on Patriot*, Jane's Intelligence Rev., Dec. 1, 2001.

17. Pub. L. 107-56.

of the Department of Justice with respect to suspected terrorism offenses, created a number of new terrorism, money laundering, and currency offenses, and increased the statutory maximum penalties for certain pre-existing offenses.

1. *Title II: New Investigative Tools*

The Act provides for significant increased authority to "intercept wire, oral, and electronic communications" relating to terrorism.[18] The Act provides that investigators can obtain a wiretap order to investigate felony violations of 18 U.S.C. § 1030, which consists of "computer fraud and abuse offenses."[19] Section 210 of the Act contains amendments clarifying that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for an account with a communications provider, "including any credit card or bank account number."[20] This information may prove particularly valuable in identifying the users of Internet services, especially where a company does not verify its users' biographical information. Also noteworthy is the provision in section 216 of the Act that grants federal courts the authority to compel assistance from any communications provider within the United States in order to effect a pen register/wiretap order.[21] Thus, when a federal prosecutor obtains an order to trace calls made to a telephone within the prosecutor's district, the order applies not only to the local carrier serving that line, but also to other providers, such as long-distance carriers and regional carriers in other parts of the country that may carry the call.

Similarly, section 219 provides that in domestic or international terrorism cases a search warrant may be issued by a magistrate judge in any district in which activities related to the offense have occurred for a search of persons or property located within or outside of that district. Section 220 likewise amends 18 U.S.C. § 2703 to allow investigators to use section 2703 warrants for e-mail to compel the production of records outside the district in which the court is located. This enables courts with jurisdiction over a case to compel evidence directly without having to involve agents, prosecutors, and judges in different districts.[22] These provisions, therefore, alleviate an enormous administrative burden that created unnecessary delays in investigating terrorist networks that spanned a number of districts.

2. *Title III: Enhanced Due Diligence Requirements*

Title III of the Act provides for a variety of counter money laundering measures, increased due diligence provisions for banks and financial institutions, and strengthens anti-counterfeiting and currency protection measures. In Title III, Congress significantly expanded and changed the responsibilities of United States financial institutions with respect to countering money laundering and terrorist activities. Significantly, section 315 of the Act expands the list of predicate offenses for money laundering. Until the Act, the only foreign crimes listed under 18 U.S.C. §§ 1956 and 1957 as predicate offenses for money laundering were drug trafficking, bank fraud, and certain crimes of violence including murder, kidnapping, robbery, extortion, and offenses involving the use of explosives.[23] Section

18. *See id.* § 202.

19. *Id.* (This provision is subject to the sunset provision of § 224, and shall cease to exist December 31, 2005).

20. 18 U.S.C. § 2703(c)(2)(F) (2001).

21. 18 U.S.C. § 3123 (2001).

22. This section is subject to the sunset provision and will cease to exist December 31, 2005.

23. *See* 18 U.S.C. § 1956(c)(7)(B) (2001).

315 expands the list of predicate offenses (also known as specified unlawful activities) to include any crime of violence, bribery of a public official or misappropriation of public funds, smuggling munitions or technology with military applications, and any "offense with respect to which the United States would be obligated by a multilateral treaty" to extradite or prosecute the offender. This expansion makes it possible to prosecute any person who conducts a financial transaction in the United States involving the proceeds of such offenses, and makes it an offense to send any money from any source into or out of the United States with the intent to promote one of these foreign offenses.

One of the most important responsibilities imposed on financial institutions under Title III is that of additional due diligence standards for financial institutions when opening or maintaining correspondent accounts for three categories of foreign banks: (1) foreign banks operating under an offshore banking license; (2) banks licensed by a foreign country designated as noncooperative with international anti-money laundering principles or procedures by an organization or intergovernmental group of which the United States is a member (and the United States concurs with that designation); and (3) foreign banks operating under a license issued by a foreign country designated by the United States Treasury Secretary as warranting special measures due to money laundering concerns. The enhanced due diligence policies must, at a minimum, ensure that domestic financial institutions take reasonable steps to (1) ascertain for any designated respondent bank (whose shares are not publicly traded) the identity of each of the owners of the foreign bank, and the nature and extent of each owners' ownership interest; (2) engage in enhanced scrutiny of the correspondent account to guard against money laundering, and file reports on any suspicious transactions; and (3) determine whether the foreign bank provides correspondent accounts to other foreign banks, and if so, the identity of those second tier banks and related due diligence requirements under 31 U.S.C. § 5318(i), paragraph one.

Paragraph three of section 5318(i) sets forth certain minimum due diligence standards for private banking accounts of non-United States persons that are maintained at domestic financial institutions. In such situations, the financial institution must take reasonable steps to (1) determine the identity of the nominal and beneficial owners of, and the source of the funds deposited into the account; and (2) perform enhanced scrutiny of a private banking account that is maintained for a senior political figure, an immediate family member or close associate in order to detect and report transactions that may involve the proceeds of foreign corruption. Furthermore, in section 313, certain "covered financial institutions"[24] are prohibited from establishing or maintaining a correspondent account in the United States for a bank that does not have a "physical presence" in any country, e.g., a shell bank. Additionally, this section requires covered financial institutions to take reasonable steps to ensure that its correspondent accounts with foreign banks, maintained in the United States for those foreign banks, are not being used by those banks to provide indirectly banking services for shell banks.[25]

24. 31 U.S.C. § 5312(a)(2) (2001). The term "covered financial institutions" means (1) an insured bank as defined in Section 3(h) of the Federal Deposit Insurance Act; (2) a commercial bank or trust company; (3) a private banker; (4) an agency or branch of a foreign bank in the United States; (5) an insured institution as defined in Section 401(a) of the National Housing Act; (6) a thrift institution; and (7) a registered broker or dealer under the Securities Exchange Act of 1934.

25. 31 U.S.C. § 5318(j) (2001).

Congress also addressed the issue of currency smuggling. Section 371 of the Act creates a new offense for bulk cash smuggling, making currency smuggling a criminal offense equivalent to smuggling firearms, jewels, or counterfeit merchandise. Specifically, the new statute at 18 U.S.C. § 5332 makes it an offense for any person with the intent to evade a currency reporting requirement under 18 U.S.C. § 5316 to conceal more than $10,000 in currency and to transport or attempt to transport the currency into or out of the United States. The new statute also provides for criminal forfeiture of the property involved in the offense, including a personal money judgment if the forfeitable property cannot be found and the defendant lacks sufficient substitute assets to satisfy the forfeiture judgment.[26]

3. *Title VIII: Amending the Definition of Terrorism*

A federal crime of terrorism is any one of thirty-eight statutorily listed predicate offenses that, generally speaking, was committed with a political motive.[27] Notably, the Act added certain offenses to the list of predicate offenses, including new computer offenses at 18 U.S.C. § 1030; offenses related to biological and chemical weapons at 18 U.S.C. § 175b and 229; offenses related to killing or attempted killing during an attack on a federal facility with a dangerous weapon at 18 U.S.C. § 930; wrecking trains, 18 U.S.C. § 1992; terrorist attacks and other acts of violence on mass transportation systems, 18 U.S.C. § 1993; and harboring terrorists, 18 U.S.C. § 2339. The Act also adds a definition of domestic terrorism to the international terrorism definition in 18 U.S.C. § 2331.

The definition of a federal crime of terrorism serves (1) to delegate primary investigative authority into such offenses to the Attorney General of the United States, and the Secretary of the Treasury at the request of the Attorney General,[28] and (2) to provide the motivational requirements for a significant sentencing enhancement in the Federal Sentencing Guidelines.[29] Thus, the amended definition expands both the investigative authority of the Attorney General, as well as increases the number of offenses that may qualify for the terrorism-sentencing enhancement.

B. The Sentencing Commission's Ongoing Counterterrorism Efforts

The Sentencing Reform Act provisions of the Comprehensive Crime Control Act of 1984 created the United States Sentencing Commission. It is an independent agency in the judicial branch of government, and its principle purposes are to (1) establish sentencing policies and practices for the federal courts, including promulgating sentencing guidelines "for use of a sentencing court in determining the sentence to be imposed in a criminal case"[30]; (2) advise and assist Congress and the Executive Branch in the development of effective criminal justice policy; and (3) collect, analyze, conduct research, and interpret a broad array of data and information regarding offenders and their sentences in order to inform Congress, the executive branch, the federal courts, criminal justice practitioners, the academic community, and the public at large about issues and trends pertaining to the federal criminal justice system.[31] Given that nearly 60,000 individual offenders and over

26. The statute features a five-year maximum sentence of imprisonment.
27. 18 U.S.C. § 2332(g)(5)(B) (2001).
28. *See id.* § 2332(f).
29. *See* USSG § 3A1.4.
30. 28 U.S.C. § 994(a)(1) (2001).
31. *See* USSG ch.1, pt. A.

300 organizations were sentenced under the Federal Sentencing Guidelines last year alone, the work and research of the Commission is of paramount importance for understanding the effectiveness of the Federal Sentencing Guidelines on reducing crime and achieving just sanctions.[32]

1. *The Nuclear, Biological and Chemical Weapons Team*

On November 1, 2001, just weeks after the first official anthrax case made headlines, new sentencing guidelines went into effect applicable to offenders convicted of conspiring, threatening, attempting to use, or actually using nuclear, biological or chemical weapons. These new guidelines also strengthened existing guidelines concerning the importation and exportation of such weapons and technologies. These guidelines, sent to Congress May 1, 2001, were the result of several years of research and collaboration with, among others, the Department of Justice, the Federal Bureau of Investigation, and the Customs Service. The guidelines responded in part to a "Sense of Congress" provision urging an increase in penalties for importation and exportation offenses involving nuclear, biological and chemical weapons, materials, and technologies.[33]

The Attorney General[34] had joined Congress in urging the Commission to increase penalties for these offenses, and also urged the Commission to draft guidelines for the new biological and chemical weapons offenses enacted at 18 U.S.C. §§ 175 and 229 (implementing the Biological Weapons and Anti-terrorism Act and the International Chemical Weapons Convention). The Attorney General asked for guidelines that would provide deterrence and punishment that would be "sufficiently clear, certain, and proportionate to the potential harm caused by the activity."[35]

The Sentencing Commission responded by chartering an interdisciplinary team to review key congressional hearing transcripts and by interviewing commissioners and staff of the President's Commission on Critical Infrastructure Protection, as well as by interviewing the staff at the United States Customs Service for information on biological agents and precursor chemicals listed by that agency. This staff work suggested that a wide range of criminal conduct might be implicated, ranging from the mailing of hoax biological agents to international operations involving the importation of nuclear materials.

The team then met with experts from the Department of Justice and the Federal Bureau of Investigation to discuss the types of conduct and circumstances that would likely be involved in these types of offenses. As a result of this extensive review, the Commission promulgated guidelines providing for graduated punishment. Among the factors in determining the ultimate sentence is whether the offense was intended to injure the United States, aid a foreign nation or foreign terrorist organization, or whether the offense was a threat that did not otherwise involve any conduct evidencing an intent or ability to carry out the threat.

Additional punishment accrues if the offense involved certain chemicals, biological agents, or nuclear materials. Increases also are provided if the offense resulted in death or

32. *See* UNITED STATES SENTENCING COMMISSION, 2000 SOURCEBOOK OF FEDERAL SENTENCING STATISTICS, fig. A.

33. National Defense Authorization Act of 1997, Pub. L. No. 104–201, § 1423 (1996).

34. The Department of Justice addressed these sentencing issues in the Attorney General's Five-Year Interagency Counter-Terrorism and Technology Crime Plan submitted to Congress in 1998.

35. *Id.*

injury, disruption of public, governmental, or business functions, or substantial expenditure of funds to decontaminate or otherwise respond to the offense. Sentences under this guideline provision range from forty-one to fifty-one months imprisonment for a threat to use anthrax (where the threat did not involve any conduct evidencing an intent or ability to carry out the threat) to life imprisonment for an offense committed with intent to injure the United States, aid a foreign nation, or aid a foreign terrorist organization.

2. *The Terrorism Team*

The anti-crime agenda of the 107th Congress was reshaped by the events of September 11, as was the agenda of the Commission. The Commission responded to the enactment of the USA PATRIOT Act by putting together a team to examine the Commission's treatment of terrorism offenses and to respond to the new provisions of the Act. In January 2002, the Commission published in the *Federal Register* draft amendment language and issues for public comment.[36] The Team worked closely with experts in the field to determine the most appropriate way to sentence different types of terrorism offenses, with the goal of sending amendments to Congress on May 1, 2002. On April 5, 2002, less than seven months after September 11, the Commission voted to promulgate a comprehensive Terrorism Amendment package that amends various provisions of the guidelines and, barring congressional action to the contrary, will take effect on November 1, 2002. The Terrorism Amendment thus constitutes an extremely rapid response by the Commission to the most comprehensive anti-terrorism bill passed in our nation's history, and furthermore, sets the groundwork for any future action the Commission may wish to undertake with respect to terrorism offenses.

Most commentators agree that even the most severe penalties will not deter terrorists, nor can dogmatic terrorists be rehabilitated. Nevertheless, severe penalties are important for two primary reasons: first, to ensure that terrorists receive the punishment they deserve, and second, to prevent future terrorist acts by incapacitating terrorists—in essence, incapacitation through incarceration. In the next section we discuss how the sentencing guidelines for organizations can work to prevent terrorism by fostering and promoting detection and early intervention through due diligence measures. Thus, where the sentencing guidelines for individuals may achieve incapacitation through incarceration, the organizational guidelines may achieve incapacitation through detection and prevention, which, in the grand scheme of things, may be a more effective counter-terrorism measure.

II. Corporate Crime and Compliance

A. The Misuse of the Corporate Entity to Facilitate Terrorism

The Organisation for Economic Co-Operation and Development (OECD)[37] recently published its "Report on the Misuse of Corporate Vehicles for Illicit Purposes."[38] According to the Report:

36. *See* Sentencing Guidelines for United States Courts, 67 Fed. Reg. 2456–2475 (Jan. 17, 2002).

37. The OECD, created on September 30, 1961, consists of several member countries working together "to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the developmnet of the world economy." Organisation for Economic Co-Operation and Developmnet, *Preface to* Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes (2001).

38. *Id.*

> While corporate vehicles play an essential role in the global economic system, these entities, may under certain conditions, be misused for illicit purposes, including money laundering, bribery/corruption, hiding and shielding assets from creditors, illicit tax practices . . . disclosure requirements, and other forms of illicit behavior.[39]

Numerous recent reports indicate that al Qaeda, Hamas, and other terrorist organizations have received and continue to receive funding through the use of charitable organizations and corporations. Consequently, the United States Treasury Department's Office of Foreign Assets Control (OFAC),[40] pursuant to Executive Order 13224 issued by the President on September 23, 2001, has frozen the assets of dozens of organizations and individuals suspected of supporting terrorism, including many organizations with rather innocuous names, e.g., the Wafa Humanitarian Organization, Al-Nur Honey Press Shops, Rabita Trust, Al-Barakat Investments, Barakat Refreshment Company, and Barakat Computer Consulting.[41]

In order to minimize the possibility of organizations being used for illicit purposes, including the financing and facilitation of terrorist activities, the OECD advocates the adoption of the following three fundamental principles: (1) organizations shall maintain publicly available records of beneficial ownership and control of the organization; (2) organizations shall maintain proper oversight and ensure the integrity of such records; and (3) organizations shall ensure that non-public information on beneficial ownership and control is shared with governmental authorities, both domestically and internationally, in order to facilitate investigations of illicit activities, while respecting the fundamental legal principles of the jurisdiction wherein the investigation occurs.[42]

As Hong Kong's Chief Secretary, Donald Tsang, recently stated in an opening address to a meeting of OECD's Financial Action Task Force on Money Laundering (FATF),[43]

---

39. *Id.* at 7.

40. OFAC's mission statement reads as follows:

> The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations and international narcotics traffickers based on U.S. foreign policy and national security goals. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFFICE OF FOREIGN ASSET CONTROL, MISSION, *available at* http://www.ustreas.gov/ofac/.

41. *See* Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism, Exec. Order No. 13224, 66 Fed. Reg. 49,079 (2001), *available at* http://www.ustreas.gov/ofac/tl11ter.pdf.

42. *See id.*

43. The FATF

> is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering—the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilised in future criminal activities and from affecting legitimate economic activities.
>
> The FATF currently consists of 29 countries and two international organisations. Its membership includes the major financial centre countries of Europe, North and South America, and Asia. It is a multi-disciplinary body – as is essential in dealing with money laundering – bringing together the policy-making power of legal, financial and law enforcement experts.

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, THE FORTY RECOMMENDATIONS 1 (2000), *available at* http://www1.oecd.org/fatf/pdf/40Rec_en.pdf.

"[t]o fight international and criminal organizations linked to terrorism, the most potent weapon is to cut off their lifeline, their sources of funding."[44] Accordingly, the FATF has promulgated recommendations intended to achieve just that end. On October 31, 2001, FATF issued its "Special Recommendations on Terrorist Financing," which, in addition to FATF's Forty Recommendations on Money Laundering,[45] "set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts."[46] The Special Recommendations are as follows:

1. Ratify and implement the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism;
2. Criminalize the financing of terrorism and associated money laundering;
3. Freeze and confiscate terrorist assets;
4. Report suspicious transactions related to terrorism;
5. Facilitate international cooperation through mutual legal assistance treaties or similar mechanisms;
6. License or register all entities providing a service for the transmission of money or value;
7. Require financial institutions and money remitters to include accurate originator information and to perform enhanced scrutiny and monitor for suspicious activities; and
8. Review the adequacy of laws and regulations that relate to non-profit organizations that may be exploited for terrorist purposes.[47]

B. Detecting and Preventing Criminal Activity

With respect to corporate crime generally, the United States long has been at the forefront of regulating and, as discussed below, incentivizing good corporate conduct. Chapter Eight of the Federal Sentencing Guidelines pertains exclusively to the sanctioning of organizations for all federal felony and Class A misdemeanor offenses.[48] They have been in effect for over a decade, and have proven to be enormously influential on organizational behavior both in terms of regulatory law and business ethics.[49]

Perhaps the most influential aspect of the organizational guidelines is the essential role of compliance programs in the sentencing process.[50] The United States, unlike many foreign jurisdictions, recognizes that organizations can be held criminally culpable for the acts of their agents. To be sure, such organizations include, corporations, but non-profits, partnerships, pensions funds and trusts, and even municipalities. Although "corporations have neither bodies to be punished, nor souls to be condemned,"[51] they do have property to be

44. Elaine Kurtenbach, *Countries Discuss Ways to Combat Financing of Terrorism, Money Laundering*, Assoc. Press, Jan. 29, 2002.

45. *See* Financial Action Task Force on Money Laundering, *supra* note 43.

46. Financial Action Task Force on Money Laundering, Special Recommendations on Terrorist Financing 1 (Oct. 31, 2001), *available at* http://www1.oecd.org/fatf/SRecsTF_en.htm.

47. *Id.*

48. *See* USSG ch. 8.

49. For a comprehensive review of the organizational guidelines and their effect on business law and ethics, see The Honorable Diana E. Murphy, *The Federal Sentencing Guidelines for Organizations: A Decade of Promoting Compliance and Ethics*, 87 Iowa L. Rev. 697 (2002).

50. *See id.* at 707–14.

51. The Oxford Dictionary of Quotations 550 (3d ed. 1979) (*quoting* Edward, First Baron Thurlow). This statement by Baron Thurlow sometimes is quoted as "Did you ever expect a corporation to have a conscience, when it has no soul to be damned, and no body to be kicked?" *Id.*

taken in the form of fines and forfeitures. This fact is shown by two primary purposes of Chapter Eight: to "provide just punishment, [and] adequate deterrence" for organizational criminal offenses through the imposition of significant fines and mandatory restitution to victims.[52] In fact, organizations can be sentenced to "death" under Chapter Eight if they primarily were created for a criminal purpose.[53]

Fines alone, however, even relatively significant ones, often are not enough to *prevent* future criminal conduct inasmuch as fines do nothing in themselves to detect the occurrence of criminal activity. Of course, significant fines may deter organizations from engaging in criminal activity, or allowing themselves to unwittingly facilitate the same. Nevertheless, the mere threat of economic sanctions cannot be expected necessarily to change an organization's culture or ethos, i.e., "the dynamic of many individuals working together toward corporate goals."[54] The possibility of fines, or even the actual imposition of them on organizations, may just be viewed by offending organizations as the cost of doing business.[55] Consequently, this is why the Organizational Guidelines also are designed primarily to "provide incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct."[56]

The main incentive for having in place prior to criminal conduct effective compliance programs is the possibility of receiving a significant fine reduction. Although compliance programs are designed to prevent and detect criminal conduct, the Sentencing Commission early on made a policy decision that the occurrence of criminal conduct does not *automatically* preclude recognizing the effectiveness of a program: effectiveness does not necessarily require perfection.[57] Another, perhaps more significant, incentive for having an effective compliance program is that it may serve to move prosecutors to decline prosecution,[58] or even, in some cases, to shield directors and officers from personal civil liability.[59]

Although some might cynically refer to compliance programs as nothing more than insurance policies, they are better conceptualized as the conscience of the organization. An organization, after all, is a good citizen not because it buys insurance against tragic or unforeseen consequences that may result from its conduct, but because it exercises the diligence due the public at large to ensure that it complies with all relevant laws and regulations, *and in addition*, fosters an air of responsibility and competence throughout the organization.[60]

52. USSG ch. 8, intro. comment.

53. USSG § 8C1.1 (requiring complete and total divestiture of organization assets if organization operated primarily for a criminal purpose or by criminal means).

54. Pamela H. Bucy, *Corporate Ethos: A Standard for Imposing Corporate Criminal Liability*, 75 MINN. L. REV. 1095, 1099 (1991).

55. *See* Murphy, *supra* note 49, at 701 (noting the Commission's and Congress' concern that prior to the organizational guidelines, fines often did "little to deter corporate crime").

56. USSG ch. 8, intro. comment.

57. *Id.* at § 8A1.2, cmt n.3(k) (2001) ("Failure to prevent or detect the instant offense, by itself, does not mean that the program was not effective.").

58. *See* Memorandum from Deputy Attorney General, Eric Holder, to All Component Heads and United States Attorneys, Bringing Criminal Charges Against Corporations (June 16, 1999), *available at* http://www.usdoj.gov/criminal/fraud/policy/Chargingcorps.html;Murphy, *supra* note 49, at 711–14.

59. *See In re* Caremark Int'l Inc., 698 A.2d 959 (Del. Ch. 1996); Murphy, *supra* note 49, at 711–14.

60. *See* Judge Richard P. Conaboy, *Welcome and Conference Overview*, *in* UNITED STATES SENTENCING COMMISSION, CORPORATE CRIME IN AMERICA: STRENGTHENING THE "GOOD CITIZEN" CORPORATION 10 (1995) (stating that "[o]ften, corporate crime appears to be the result of a failure to establish values and modes of conduct that are based on clear, ethical, and moral standards.").

The Organizational Guidelines identify the following seven criteria that, at a minimum, a compliance program must meet in order to be deemed effective:

(1) Establish compliance standards and procedures reasonably capable of reducing the prospect of criminal conduct.
(2) Assign high-level personnel overall responsibility to oversee compliance with such standards and procedures.
(3) Use due care not to delegate substantial discretionary authority to individuals whom the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activities.
(4) Take steps to communicate effectively its standards and procedures to all employees and other agents, e.g., by requiring participation in training programs or by disseminating publications that explain in a practical manner what is required.
(5) Take reasonable steps to achieve compliance with its standards, e.g., by utilizing monitoring and auditing systems reasonably designed to detect criminal conduct, and provide an anonymous reporting system.
(6) Enforce standards consistently through appropriate disciplinary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense.
(7) After an offense has been detected, the organization must have taken all reasonable steps to respond appropriately to the offense and to prevent further similar offenses – including any necessary modifications to its program to prevent and detect violations of law.[61]

Largely as a result of the central role effective compliance programs play in the Organizational Guidelines, more industries are adopting and standardizing compliance programs to fit the needs of their particular enterprises.[62] When assessing whether a compliance program is "effective," the Organizational Guidelines direct the courts to also consider industry practice and standards. According to the Organizational Guidelines, "[a]n organization's failure to incorporate and follow applicable industry practice or the standards called for by any applicable governmental regulation weighs against a finding of an effective program to prevent and detect violations of law."[63]

This additional factor perhaps is the most important of all the compliance program criteria inasmuch as it provides a perspective from which to assess whether the offending organization was a "rotten apple." But this additional factor will remain meaningless and ineffective unless industries move toward adopting and defining the other seven criteria within the context of their particular industries. Otherwise, the "rotten apple" may just be an indicator of a "rotting barrel." With that in mind, in the next section we advocate the adoption of "Globalized Diligence," which, at its heart, requires the standardization of "Know Your Customer" and "Know Your Employee" provisions, as well as the development of timely and efficient mechanisms to share information pertaining to potential criminal activities with others within the private sector (private-to-private), as well as with relevant government agencies (private-to-public and public-to-private).

III. Recognizing a New Paradigm: Globalized Diligence

In light of OECD's call to organizations to share ownership and control information with both the private and public sectors, as well as FATF's call to the international com-

61. *See* USSG § 8A1.2, cmt. n.3(k).
62. *See id.* pt. IV.
63. *See* USSG § 8A1.2, cmt. n.3(k).

munity to provide regulations to facilitate the reporting of suspicious activities by the private sector, the financial and telecommunications industries together must work diligently and quickly to ensure that their practices and standards meet these goals in letter and spirit. With respect to the ongoing war on terrorism, the paradigm has shifted in the financial and telecommunications industries from competition to national security, which requires greater diligence and cooperation within these industries in order to cut off the tools that make terrorism possible. No longer can the financial and the telecommunications industries focus their compliance programs solely on auditing and compliance, but they must expand their programs to ensure that their member organizations do not become the unwitting tools of terrorists and international criminals.

In the words of Professor George Brenkert, "[t]he expanding globalization of business has brought with it the increased importance of an international business ethics."[64] The ethics now called for is beyond mere compliance; it requires the private sector collectively to develop appropriate standards and "best practices" consistent with globalized diligence, and would-be good corporate citizens to remove barriers to cooperation with each other and with national governments. To be sure, "[w]e have not come here to preach to anybody about what their moral standards should be, but it would be foolhardy not to recognize that the kind of programs that we're talking about . . . must be based on clear ethical and moral standards or they have no chance of success."[65]

In this section, we review three fronts in the war on terrorism where increased diligence now is due with respect to ethics and compliance programs: the financial front, the cyber front, and the personnel front.

A. The Financial Front

In perhaps the most memorable scene in the motion picture *All the President's Men*, *Washington Post* reporter Bob Woodward (played by Robert Redford) surreptitiously meets the mysterious "Deep Throat" in a darkened parking structure to glean information about the ongoing Watergate scandal. From out of the shadows, "Deep Throat" whispers to Woodward the key to unraveling the scandal: "Follow the money!" Recognizing the key role money plays in the War on Terrorism, "[t]he President's first strike in the war against terror was not with a gun or a missile—the President's first strike was with his pen as he took action to freeze terrorist finances and disrupt their pipelines for raising and moving money in the future."[66] According to President Bush, the United States has "put the world's financial institutions on notice: if you do business with terrorists, if you support them or sponsor them, you will not do business with the United States of America."[67] Not only will such an organization be precluded from doing business with the United States, but it could either be totally divested of its assets[68] or, at the very least, have such assets frozen. Indeed,

64. George C. Brenkert, *Trust, Morality and International Business*, *in* Ethical Issues in Business: A Philosophical Approach 118 (Thomas Donaldson et al. eds., 2002).

65. *See* Conaboy, *supra* note 60, at 10.

66. The Coalition Information Centers, *supra* note 14, at 9.

67. *Id.*

68. *See* USSG § 8C1.1 (2001) ("If, upon consideration of the nature and circumstances of the offense and the history and characteristics of the organization, the court determines that the organization operated primarily for a criminal purpose or primarily by criminal means, the fine shall be set at an amount (subject to the statutory maximum) sufficient to divest the organization of all its net assets."). This provision of the Organizational Guidelines commonly has been referred to as the "corporate death penalty." *See* USSG § 8C1.1.

since the inception of the war on terrorism, "[t]he assets of at least 153 known terrorists, terrorist organizations, and terrorist financial centers have been frozen in the U.S. financial system" totaling over $66 million worldwide.[69]

In light of Title III of the USA PATRIOT Act,[70] the Treasury Department issued "three proposed rules, one interim rule and one final rule for financial institutions and businesses regarding compliance with anti-money laundering provisions of the USA PATRIOT Act."[71] One of the proposed rules "implement[s] the provision in the USA PATRIOT Act that requires trades and businesses to report cash transactions of more than $10,000 (or two or more related transactions involving more than $10,000) and certain transactions involving monetary instruments to Treasury's Financial Crimes Enforcement Network."[72] Another of the proposed rules codifies interim guidance to banking institutions on complying with certain anti-money laundering provisions of the Act that Treasury had issued on November 20, 2001. One of the provisions of the Act "prohibits certain U.S. financial institutions from providing correspondent accounts to foreign shell banks" and requires those institutions to "take reasonable steps to ensure that foreign banks not use correspondent accounts to indirectly provide banking services to foreign shell banks."[73]

B. The Cyber Front

Cyberspace now is more relevant to the financial world than even "real-space." Indeed, far more transactions occur on-line or electronically than at a teller's window. Consequently, maintaining the integrity of our financial system requires guarding cyberspace from so-called cybercrime, and its more nefarious manifestation, cyberterrorism. Moreover, the integrity of our national infrastructure itself depends on the integrity of cyberspace given that virtually every critical function of our government and our economy operates through it. Not surprisingly, therefore, "[t]here is concern that this reliance on computers and computer networks raises the vulnerability of the nation's critical infrastructures to 'cyber' attacks."[74] Accordingly,

> A national protection plan cannot be accomplished without private and public partnerships because many of the key targets for cyberattack—power and telecom grids, financial flows, transportation systems—are in private hands. Such a partnership is a prerequisite of designing and developing a defense system to protect both the private and the public sectors against critical infrastructure attack.[75]

Indeed, "[t]he nature of the medium suggests that, as in the early American frontier, the

69. *See* The Coalition Information Centers, *supra* note 14, at 9.

70. *See infra* II.B.

71. Press Release, Department of the Treasury, Treasury Department Issues Regulations on Compliance with USA PATRIOT Act (Dec. 20, 2001), *available at* http://www.treas.gov/press/releases/po887.htm.

72. *Id.*

73. *Id.*

74. *See* John D. Moteff, Summary, Congressional Research Service, Critical Infrastructures: Background, Policy, and Implementation (updated Dec. 14, 2001), *available at* http://www.fpc.gov/CRS_REPS/cii1214.pdf.

75. William H. Webster & Arnauld de Borchgrave, Foreword to Center for Strategic & International Studies, CYBERCRIME . . . CYBERTERRORISM . . . CYBERWARFARE . . . Averting an Electronic Waterloo (1998), *available at* http://www.csis.org/pubs/cyberfor.html.

government may be poorly positioned to combat cybercrime."[76] Rather, "[p]otential cybercrime victims, such as financial institutions, may be the most efficient front-line defense against cybercrime. This same rationale may apply equally to third-party participants, such as Internet service providers (ISPs), which may not be victims, but rather unwitting participants in criminal activity."[77]

As with the financial industry, the telecommunications industry must avail itself of appropriate and efficient methods for identifying potential criminal or terrorist activities. Although cyberspace may provide an efficient and anonymous means to create extreme havoc, it also can be used as a tool by the private sector for investigating and monitoring suspicious transactions and coordinating appropriate responses.

And just as due diligence standards for the financial industry now require greater scrutiny not just of the money flowing in, but the money flowing out, so too the telecommunications industry must exercise greater scrutiny to ensure that hard products—computers, satellite phones, satellite navigational tools, as well as soft products—encryption software, do not fall into the wrong hands. After all, "[w]ith his hectic, on-the-go lifestyle, no self-respecting terrorist can function without a computer that fits comfortably on an airplane tray table."[78] By denying terrorists access to such technology, future terrorists hopefully will remain grounded.

C. Personnel Front

We have been arguing that the current war on terrorism cannot be won without increasing both due diligence standards and cooperative standards of industries and organizations. But the success of such efforts ultimately rests, of course, with the so-called "human element." Dr. Jerrold Post, a noted expert on cybercrime and terrorism, has noted that the largest threat comes not from external sources, but from the malicious insider.[79] Thus, in addition to the heightened due diligence and reporting standards that the financial and telecommunications industries must adopt with respect to external transactions and events, they must also work to adopt comprehensive hiring, screening, and training standards for employees in their industries. In short, the industries, and not just the organizations within them, must adopt standards of "due care not to delegate substantial discretionary authority to individuals whom the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activities."[80]

IV. The Co-operative Requirements of Globalized Due Diligence

As discussed above, sections 312 and 314 of the USA PATRIOT Act provide for mechanisms that facilitate the cooperation of the private sector with other members of the private sector, as well as with government. The aim of the cooperation is information exchange.

76. Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 Geo. Mason L. Rev. 237, 240 (2000).

77. *Id.*

78. Barak Jolish, *The Encrypted Jihad: We Can't Stop Terrorists from using Uncrackable Codes. So We Shouldn't Even Try, at* http://www.salon.com/tech/feature/2002/02/04/terror_encryption/print.html.

79. *See also* Michael A. Vatis, Statement before the Senate Committee on Commerce, Science and Transportation Subcommittee on Communications (Mar. 8, 2000) (stating that "[t]he disgruntled insider (a current or former employee of a company) is a principal source of computer crimes for many companies.").

80. USSG § 8A1.2, cmt. n.3(k).

Recently, in a speech to the Computer Privacy, Policy & Security Institute, Attorney General Ashcroft noted the integral role the private sector plays in the fight against cybercrime.[81] "Our experience with *good corporate citizens* that do report crime has been excellent."[82] According to the Attorney General, success in fighting cybercrime largely depends on "the timely reporting of the events by the victims."[83] Because the private sector, almost by definition, is at the financial, electronic, and employment front lines, the war on terrorism and international crime can only be fought with the private sector's cooperation.

And this cooperation extends not just to timely reporting of suspicious activities, but must also extend to the prevention and detection of unlawful activities. As Defense Secretary Donald H. Rumsfeld stated in remarks at the National Defense University, "wars in the 21st century will increasingly require all elements of national power: economic, diplomatic, financial, legal, law enforcement, intelligence, as well as overt and covert military operations."[84] With respect to intelligence in the current war on terrorism, the private sector can provide invaluable, indeed necessary, assistance.

To be sure, neither this call for private sector assistance, nor the private sector's willingness to work for the greater good in times of national need is something new. Within the marble halls of Union Station in Washington, D.C., there sits a large, solemn plaque entitled "Lest We Forget." It reads in part as follows:

> On April 11, 1917, five days after the United States entered the World War, representatives of practically all the railroads in the country assembled in Washington in response to an invitation from the Council of National Defense . . . and unanimously adopted the following resolution:
>
> *That the railroads of the United States, acting through the Chief Executive Officers here and now assembled, and stirred by a high sense of their opportunity to be of greatest service to their country in the present national crisis, do hereby pledge themselves with the government of the United States, with the governments of the Several States, and on with another, that during the present war they will coordinate their operations in a continental railway system, merging during such period all their individual and competitive activities in an effort to produce a maximum of national transportation efficiency.*
>
> This action, the first of its kind taken by an industry in the United States, proved of inestimable value as an example of voluntary co-ordination of corporate interests for the public welfare.

Like the railroad industry at the beginning of last century, the financial and telecommunications industries at the beginning of this century should, in recognition of the fundamental paradigm shift in the duties now owed, voluntarily coordinate their interests for the public welfare in the war on terrorism.

V. Conclusion: The New Prevention Paradigm

Globalization, while increasing the economic prosperity of billions through facilitating global commerce, at the same time has increased the vulnerability of the world's economy

81. *See* Attorney General John Ashcroft, Remarks at the First Annual Computer Privacy, Policy & Security Institute (May 22, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/AGCPPSI.htm.

82. *Id.* (emphasis added).

83. *Id.*

84. Secretary of Defense Donald H. Rumsfeld, Remarks at the National Defense University (Jan. 31, 2002), *available at* http://www.defenselink.mil/speeches/2002/s20020131-secdef.html.

to terrorism. With the benefits of globalization come significant burdens. The hope that remains is that through the increased diligence and cooperation of the private sector, future terroristic activities will be detected, and thereby prevented, *before* they can come to fruition, with the result that the prosperity globalization provides will continue to flourish and the darkness that may grow from it never takes root.

In a talk at Southern Methodist University's conference on "Terrorism's Burdens on Globalization," Professor Barry Kellman spoke of a new paradigm for nations in light of the unique threats to civilization that terrorism presents, which he called the Paradigm of Prevention. According to Professor Kellman, nations no longer can deal with the threat of terrorism through a reactionary paradigm, i.e., dealing with terrorism after it has occurred. Rather, a new paradigm now exists: the paradigm of precaution and prevention. And as the private sector is at the front lines of the war on terrorism, this paradigm must also apply, and be recognized by the financial and telecommunications industries. The paradigm has shifted the diligence due from being perceived as a possibly anti-competitive cost to a requirement and commitment by the private sector to ensure that threats to our society do not again manifest into the horrors of September 11. Those industries and organizations that do not heed the call to globalized diligence could find themselves the unwitting—or worse, the indifferent—agents of evil and corruption. And they rightly should suffer significant consequences.

In his now infamous 1968 article in the *Harvard Business Review* "Is Business Bluffing Ethical?" Professor Albert Carr argued that "business . . . standards of right and wrong differ from the prevailing traditions of morality in our society."[85] Carr illustrated this point by arguing that a key manufacturer who provided master keys for automobiles to mail order customers without attempting first to ascertain whether he was selling them to car thieves, was not acting unethically.[86] According to Carr, "[u]ntil the law was changed, the key manufacturer could regard himself as being just as ethical as any other businessman by the rules of the business game."[87]

Carr, of course, was wrong to distinguish ethics in business from ethics in society. Willful blindness and negligent oversight in one context does not become acceptable in another simply because it may be profitable or expedient.[88] In all events, as we reviewed above, the law has changed so that even Carr's manufacturer cannot fall back on his wrong-headed excuse. The paradigm of prevention now is paramount. Recognizing this, the financial and telecommunications industries must quickly develop international standards and codes of conduct that foster cooperation among the private sector, as well as between the private and public sector, such that it is understood by all that the diligence due is global and that their cooperative efforts is required for the greater public good.

85. Albert Carr, *Is Business Bluffing Ethical? in* ETHICAL ISSUES IN BUSINESS: A PHILOSOPHICAL APPROACH, *supra* note 64, at 108.

86. *See id.*

87. *Id.*

88. Indeed, such willful blindness may expose a director or officer of a corporation to civil and even criminal liability. *See In re* Caremark, 698 A.2d 959 (Del. Ch. 1996); Murphy, *supra* note 49, at 711–14.