Backgrounder

Published by The Heritage Foundation

No. 2138
May 21, 2008

Fighting Terrorism, Addressing Liability: A Global Proposal

James Jay Carafano, Ph.D.

Homeland security is a global enterprise. Almost every aspect of keeping Americans safe, free, and prosperous in the face of transnational terrorism requires cooperation with friends and allies.

In some cases, this collaboration requires joint programs in which nations learn from each other by sharing best practices. The challenges are to make this cooperation efficient and effective without compromising the sovereignty of individual nations or impinging on the rights and liberties of their citizens. One area that is ripe for enhanced international cooperation is third-party liability for terrorist attacks.

The recent bitter debate between Congress and the Administration about whether to extend immunity from civil suits to telecommunications companies that cooperated with a classified government surveillance program highlights one of the knotty challenges involved in promoting public–private cooperation in the fight against terrorism.[1] Whether companies act or fail to act to prevent an act of terrorism, the courts may be asked to hold someone accountable for any damages.

In contrast to its attitude toward telecom companies, after the terrorist attacks of September 11, 2001, Congress became so concerned about rampant lawsuits over alleged failure to prevent the attacks, as well as claims of contributing to the catastrophic losses suffered in their aftermath, that it quickly passed legislation that limited third-party liability. Congress extended these protections to the airlines involved, the New York Port Authority, and the city

Talking Points

- Homeland security is a global enterprise. Almost every aspect of protecting Americans from transnational terrorism requires cooperation with friends and allies.
- The different responses from Congress regarding third-party liability reflect the struggle within government over how best to deal with legal issues that surround the nation's response to terrorist threats.
- Since 9/11, Congress has acted decisively in one area of liability protection: The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act lowered the liability risks of manufacturers that provide products and services for combating terrorism.
- Effective homeland security requires programs that make international cooperation efficient and effective without compromising national sovereignty or impinging on the rights and liberties of citizens.
- DHS and the State Department should work to engage other nations in a serious dialogue on expanding the umbrella of liability protection for effective anti-terrorism technologies to all free nations.

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/bg2138.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

government as well as the Dulles, Portland, and Boston airports.

In addition, Congress established a Victim Compensation Fund for individuals (or their families) and businesses for death, injury, and losses resulting directly from the attacks or the response at the scene. Businesses received the largest share of compensation—62 percent of the payments.[2]

These very different responses from Congress regarding third-party liability reflect the struggle within government over how best to deal with the thorny issues that surround the nation's response to terrorist threats.

Since 9/11, Congress has acted decisively and to good effect in one area of liability protection: The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act lowered the liability risks of manufacturers that provide products and services used in combating terrorism. The act, passed in 2002, protects the incentive to produce products that the Secretary of Homeland Security designates as "Qualified Anti-Terrorism Technologies." The Department of Homeland Security (DHS) has made a concerted effort to implement the program, and about 200 companies have obtained SAFETY Act certification.

The SAFETY Act provides protections to "sellers" (manufacturers, distributors, and providers) for cases under the jurisdiction of U.S. courts. Terrorism, however, is a global threat, and homeland security is a global mission. From securing the border to protecting global supply chains, virtually every aspect of preventing terrorist attacks has an international dimension that requires the United States to work effectively with friends and allies.[3] Other countries should consider similar liability-protection regimes to provide the industrial base of all free nations with incentives to develop and adopt the best tools to fight terrorism no matter where they are manufactured or employed.

The best way to promote effective international cooperation is on a bilateral basis. Nations bear the primary responsibility for protecting their citizens. In turn, nations must collaborate with one another to protect their mutual interests. The United States can contribute to this cause most effectively by continuing to develop and strengthen the implementation of the SAFETY Act and by sharing best practices and lessons learned with other countries. Meanwhile, other nations should establish their own liability-protection regimes.

Acting Safe

Since 9/11, insurance premiums for all terrorism-related risks have skyrocketed, and a gradually increasing number of firms have stopped offering terrorism insurance.[4] Many companies proved hesitant to market anti-terrorism technologies because of two concerns: the costs of potentially devastating jury verdicts should the technologies fail and the costs and scarcity of adequate liability insurance.

Congress intended the SAFETY Act to serve as a critical tool for promoting the creation, proliferation, and use of technologies to fight terrorism.[5] The act provides risk- and litigation-management protections for producers of Qualified Anti-Terrorism Technologies and other providers in the supply and distribution chain. Specifically, it created liability limitation from third-party claims for losses

1. See James Jay Carafano, Robert Alt, and Andrew M. Grossman, "Congress Must Stop Playing Politics with FISA and National Security," Heritage Foundation *WebMemo* No. 1791, January 31, 2008, at *http://www.heritage.org/Research/LegalIssues/wm1791.cfm*.
2. Lloyd Dixon and Rachel Kaganoff Stern, *Compensation for Losses from the 9/11 Attacks* (Santa Monica, Cal.: RAND, 2004).
3. James Jay Carafano and Richard Weitz, "Enhancing International Collaboration for Homeland Security and Counterterrorism," Heritage Foundation *Backgrounder* No. 2078, October 18, 2007, at *http://www.heritage.org/Research/HomelandDefense/bg2078.cfm*.
4. Richard Hillman, "Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities," testimony before the Subcommittee on Oversight and Investigations, Committee on Financial Services, U.S. House of Representatives, February 27, 2002, at *http://www.gao.gov/new.items/d02472t.pdf* (May 14, 2008).
5. *Federal Register*, Vol. 71, No. 110 (June 8, 2006), pp. 33147–33168, at *http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/06-5223.htm* (May 13, 2008).

COMPANIES THAT HAVE RECEIVED SAFETY ACT CERTIFICATION

Michael Stapleton Associates (MSA) was the first company to receive SAFETY Act certification. It received certification for its explosive-sniffing canines and SmartTech explosive-inspection system. The award to MSA represented everything that is good about the SAFETY Act: It recognized the valuable contribution of small companies in warding off terrorist attacks as well the important role carried out by bomb-sniffing dogs.

IPC International, Inc., provides security officers to retail centers across the United States. In giving SAFETY Act protections to IPC, the Department of Homeland Security acknowledged the important role that well-trained security officers play in defending the United States, particularly "soft" targets like shopping centers.

Triple Canopy, Inc., received SAFETY Act certification for its security analysis and planning services, which include vulnerability assessment as well as "red team" risk assessments. The SAFETY Act award to Triple Canopy helps to ensure that infrastructure facilities will have thoroughly vetted companies, able to offer valuable mitigation strategies and recommendations, available to them.

resulting from an act of terrorism where the technologies were deployed to help identify, deter, defend against, respond to, or mitigate the danger of a terrorist attack.

The term "Qualified Anti-Terrorism Technologies" covers a broad spectrum of products and services. Certification eligibility can be extended to:

- Threat and vulnerability assessment,
- Detection systems,
- Blast-mitigation materials,
- Screening services,
- Sensors and sensor integration,
- Threatening-object detectors,
- Decision-support software,
- Security services, and
- Crisis-management services.

The SAFETY Act also encourages the development of software and other forms of intellectual property. In 2007, certification was awarded to IBM for a software application that improves the accuracy of name searching and identity verification. Overall, the certifications that have been awarded have a broad and significant impact on the everyday security of Americans.

The certification program is managed by the DHS Directorate for Science and Technology. The Office of SAFETY Act Implementation will conduct the application review using statutory criteria to assess various technologies:

- *Technical capabilities and efficacy.* The department must establish the suitability and limitations of the product or service.
- *Economic effects of deployment vs. non-deployment.* DHS must perform a risk assessment to determine how vital deployment might be in fighting terrorism.
- *Evaluation of insurance needs.* Before a technology receives a rating as a Qualified Anti-Terrorism Technology, DHS must evaluate the amount of liability insurance to be maintained for coverage of the technology and certify that it is appropriate to satisfy claims that result from an act of terrorism. The SAFETY Act also stipulates that providers are not required to obtain insurance in excess of the maximum reasonable amount. The cost of insurance should not unreasonably distort the sales price of the technology.

The office also maintains a pre-application process so that businesses can get a fast initial opinion about whether they have the potential for certification before they undertake the time and expense of the full application process. The pre-application assessment is done at no cost to the business.

In assessing the applications, DHS considers a number of factors:

- Results from operational tests that demonstrate products' real-world performance,
- Documentation of product performance on previous deployments,
- Assessments by experts,
- Feedback from customers,
- Quality-assurance plans, and
- Audit results.

Throughout the assessment process, DHS employs safeguards to protect proprietary information and sensitive data.

The SAFETY Act provides two different levels of liability protection: designation and certification. The seller's liability for products or services that are deemed "designated technologies" is limited to the amount of liability insurance that the Department of Homeland Security determines the seller must maintain. Designation can also be obtained for promising anti-terrorism technologies that are undergoing testing and evaluation.

In addition to the benefits provided under designation, certification allows a seller of an anti-terrorism technology to assert the "government contractor defense" (if the government is immune from a lawsuit, the private contractor is too) for claims arising from acts of terrorism. Technologies that receive certification will be placed on DHS's Approved Products List for Homeland Security.[6]

SAFETY Act protection provides a number of advantages. If claims are made against Qualified Anti-Terrorism Technologies that have received a "designation," the claims can be made only in a federal court. Even if the court rules against the defendant, the plaintiff can recover damages only in proportion to the degree of fault of the technology for failure to prevent the attack. In other words, companies may only be liable for the percentage of damages proportionate to their responsibility for the harm done. Thus, if the court finds a terrorist cell 50 percent responsible for a successful attack and the technology 50 percent responsible for failing to prevent the attack, then the company providing the technology must pay only half of the damages. Plaintiffs also cannot sue for punitive damages.

Technologies that receive a "certification" have an established claim to complete liability immunity for manufacturers and their customers. They are allowed to claim the government contractor defense. SAFETY Act certification applies whether the provider delivers goods or services to government or private clients. Plaintiffs challenging this defense would have to prove the defendant guilty of "fraudulent or willful misconduct."

Keeping the SAFETY Act Safe

Although the protections of the SAFETY Act have yet to be tested in court, there are many signs that the law is working as intended. DHS took a "crawl, walk, run" approach to implementing the certification process. In its first year and a half of operation, the program approved six certifications. In fiscal year 2007, the program approved 81 applications, an 83 percent increase over all approvals attained over the previous three years. In February 2008, DHS gave its 200th approval.[7] As companies learn about the program and understand the application process and protections offered, they are lining up in growing numbers to apply—surely a sign that the private sector is gaining confidence in the program and remains keenly interested in bringing new counterterrorism technologies to the marketplace.

To satisfy the increasing demand, the Office of SAFETY Act Implementation has expanded. About 420 experts are now available to review applications, including 90 trained reviewers in seven threat areas: in cyberspace and the economy, as well as chemical, biological, explosive, radiological, and human threats.

Despite the progress that has been made, however, the future of the SAFETY Act is not secure.

6. Regulations Implementing the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, "Benefits to Your Company," June 6, 2006, at *https://www.safetyact.gov* (May 14, 2008).
7. U.S. Department of Homeland Security, Office of SAFETY Act Implementation, *The SAFETY Act*, p. 11, at *https://www.safetyact.gov* (May 14, 2008).

Congress has engaged in a bitter debate over providing immunity protections to telecommunication companies that voluntarily cooperated with the U.S. government in the Terrorist Surveillance Program.[8] Six years after 9/11, Congress has demonstrated its increasing reluctance to limit tort action—even for the purpose of reducing the threat of terrorist attacks. Opposition to a proposed Senate bill, the Protect America Act, may presage an effort to roll back private-sector liability protections.[9]

Another issue of concern is the controversy that surrounded the September 11 Victim Compensation Fund of 2001, intended to compensate victims or their families in exchange for their agreement not to sue private-sector entities.[10] After the next terrorist attack, Congress might prove reluctant to rely on similar solutions. A RAND study concluded that, "while the government programs put in place after 9/11 create a precedent for programs that might be adopted after a future attack, there is no guarantee that similar programs will be adopted in the future."[11] The next time, rather than providing tort liability protections to the private sector, Congress might prove anxious to place the issue in the hands of civil courts, which would likely result in bitter, protracted, and expensive litigation battles.

Neither DHS nor the private sector can assume that Congress will allow the SAFETY Act to stand over time. In order to keep the program moving forward and to fight off the special-interest tort lawyers who would prefer an "open field" for litigation, DHS must continue to improve the program and demonstrate its efficacy. To this end, the Department of Homeland Security should:

- **Encourage** new entrants into the SAFETY Act process, including owners of critical infrastructure facilities and operators of "soft" targets like sports stadiums, shopping malls, and amusement parks.
- **Continue** to refine the assessment process and maintain a thorough but not unduly burdensome auditing program to demonstrate the efficacy of DHS certifications.
- **Ensure** that the certification process also addresses civil liberty and privacy concerns, since many technologies are used in the surveillance and screening of U.S. citizens.
- **Carefully implement** the Developmental Testing and Evaluation Designations to avoid undermining the credibility of the SAFETY Act protections. This level of liability protection was added in the 2006 DHS final rule to give companies an incentive to invest in research and development and the testing, evaluation, and marketing of products not yet fully developed.[12]

Implementing these measures quickly and with due diligence would both enhance the credibility of the certification process and encourage more and more companies to seek SAFETY Act protections. The more widely it is employed, the less likely it is that Congress will try to scale back the program.

Going Global

In addition to moving the program forward, DHS should make a concerted effort to document best practices and lessons learned in order to share them with America's allies. In addition, other nations should establish their own liability protections. The U.S. Department of State should collaborate with the Department of Homeland Security to establish a deliberate and effective outreach program.

One potential source of outreach might be the Technical Cooperation Program (TTCP), an interna-

8. For program description, see Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview," Congressional Research Service *Report for Congress Update*, January 18, 2007, pp. 18–20, at *http://www.fas.org/sgp/crs/intel/RL31798.pdf* (May 14, 2008).
9. Andrew M. Grossman, "FISA Modernization Is Not About 'Warrantless Wiretapping,'" Heritage Foundation *WebMemo* No. 1847, March 12, 2008, at *http://www.heritage.org/Research/LegalIssues/wm1847.cfm*.
10. James R. Copland, "Tragic Solutions: The 9/11 Victim Compensation Fund, Historical Antecedents, and Lessons for Tort Reform," Manhattan Institute, Center for Legal Policy, January 13, 2005, pp. 22–24, at *http://www.manhattan-institute.org/pdf/clpwp_01-13-05.pdf* (May 14, 2008).
11. Dixon and Stern, *Compensation for Losses from the 9/11 Attacks*, p. 140.
12. *Federal Register*, Vol. 71, No. 110.

tional organization that collaborates in defense-related scientific and technical information exchange and shared research activities with Australia, Canada, New Zealand, the United Kingdom, and the United States. TTCP is one of the world's largest collaborative science and technology forums.

Outreach might focus initially on U.S. partners in Asia including Japan, Australia, New Zealand, Taiwan, South Korea, India, Hong Kong, and Singapore. Singapore is the United States' 15th-largest trading partner and ninth-largest export market. Foreign direct investment in Singapore is concentrated largely in technical service sectors; manufacturing; information; and professional scientific knowledge, skills, and processes.[13]

As national liability protection proliferates, new opportunities for international cooperation will emerge. Countries that adopt verifiably similar liability protections should extend reciprocal privileges to one another.

An expanding global web of liability protection will facilitate the proliferation of anti-terrorism technologies. The benefits would likely include:

- Security-assistance sales, lease, and grant programs that would allow DHS to assist other countries in obtaining equipment, support services, and financing for homeland security functions.
- Increased international collaboration for research, development, and sharing of security technologies, coordinated by the DHS Directorate of Science and Technology, through such instrumentalities as a new international clearinghouse for technical information.

Promoting liability-protection programs should be the centerpiece of a comprehensive global homeland security outreach program.[14]

Conclusion

For the makers of anti-terrorism technologies and their suppliers and customers, the SAFETY Act provides the means to reduce the burden of liability insurance by lowering potential liability payments from claims resulting from a terrorist attack. At the same time, the SAFETY Act program encourages businesses to engage and do what they do best—create and innovate.

The Department of Homeland Security should continue to invest in this program. Congress should fully fund the activities of the Office of SAFETY Act Implementation and not alter the authorities of DHS under the act. Finally, DHS and the State Department should work as a team to engage other nations in a serious dialogue on expanding the umbrella of liability protection for effective anti-terrorism technologies to all free nations.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. Heritage intern Gabriela Herrera contributed to this paper.

13. Office of the U.S. Trade Representative, "Singapore," at *http://www.ustr.gov/World_Regions/Southeast_Asia_Pacific/Singapore/Section_Index.html* (March 7, 2008).
14. For specific recommendations, see James Jay Carafano, Jonah J. Czerwinski, and Richard Weitz, "Homeland Security Technology, Global Partnerships, and Winning the Long War," Heritage Foundation *Backgrounder* No. 1977, October 5, 2006, at *http://www.heritage.org/Research/HomelandSecurity/bg1977.cfm*