

The NATIONAL STRATEGY FORUM REVIEW

An Online National Security Journal Published by the National Strategy Forum

Book Review: Skating on Stilts by Stewart Baker

By Richard E. Friedman

Richard E. Friedman is President of the National Strategy Forum and Publisher of the National Strategy Forum Review. He is also a Counselor to the American Bar Association Standing Committee on Law and National Security.

Stewart Baker, the author of the outstanding book, *Skating on Stilts*, is a member of a small group of gifted lawyers who serve America and the private sector with great distinction. Typically, they are in high echelon government service for several years, return to their private practice, and often answer the call to public service again. Stewart Baker has specialized in electronic communication law: he was General Counsel of NSA, and he became the first person to serve as Assistant Secretary for Policy of the U.S. Department of Homeland Security (DHS) shortly after Secretary Michael Chertoff took office. The relatively new DHS had been cobbled together from many national security agencies by the first DHS Secretary, Tom Ridge.

Mr. Baker was assigned to identify, conceptualize, negotiate, and resolve a daunting array of problems that are detailed in this book:

- Airline travel security
- Port Security
- Data Collection
- Cybersecurity
- Visa Waivers
- Bioterrorism
- Financial Transaction Security

This book is a must-read for Americans who want to be informed about our national security and their personal safety. Some books rely upon tedious detail; however, the detail in Mr. Baker's book provides the necessary background for a sweeping panoramic view of several important aspects of U.S. national security.

The author identifies friends and foes of U.S. national security who are neither al Qaeda nor Taliban. The surprising adversaries are the ACLU and the privacy lobby, the European Commission, Congress and its staff bureaucracy, and, frequently, the turf-centric national security agencies, including the NSA, NSC, FBI, DOD, CIA, and trade-oriented U.S. commercial agencies. The media, in Mr. Baker's view, are frequently neither honest brokers nor purveyors of accurate information regarding national security matters.

Information technology developed rapidly in the early 1970s and changed the way America handled its national security business. The number of transistors that can be placed on a computer chip cheaply doubles every 18 to 24 months. Shortly after 9/11, the American public became aware of the need to "connect the dots" that might have prevented the 9/11 terrorist attacks. The security gaps have been chronic since the 1970s and U.S. information security remains far behind the power curve as we grapple with cybersecurity today.

By law, since 1947 there has been a wall between foreign intelligence and domestic intelligence gathering for criminal prosecutions. The CIA and FBI were prevented from sharing information. The consequence was that known terrorists could plan and exchange information and avoid government interference even though government national security agencies had undigested, relevant information in their possession.

The American civil liberties establishment has been hugely successful in their privacy campaign – the equivalent of the success of the gun lobby. The issue is whether civil liberties and privacy concerns are real or hypothetical, and how they enhance or impede government national security undertakings. Mr. Baker's view is that the civil liberties establishment, supported by an uncritical media, has successfully opposed new security measures based upon their belief that they are an intrusion on civil liberties, although many of these concerns have been demonstrated to be hypothetical or erroneous.

Congress, backed by President Bush II's initiative to tear down the intelligence and criminal investigation gathering wall, passed three laws that require sharing of terrorist data among the intelligence and law enforcement community. As this wall crumbled, another wall was erected by the European Commission.

For many years, the U.S. had collected trans-Atlantic passenger information data. In 1995, the European Commission (E.C.) acted to prevent data from being transferred to the U.S., because it deemed U.S. data protection to be inadequate. Because of the international scope of the problem, the E.C. gained allies at the NSC and DOS. The DHS position was that the European privacy concerns had constrained the ability of counterterrorism officials to prevent acts of terrorism.

The detailed narrative of Mr. Baker's negotiations with the E.C. and recalcitrant U.S. agencies is fascinating. Hurrah for DHS and Mr. Baker as he takes the reader step by step through the tedious and intriguing negotiation process that resulted in the E.C.'s abject surrender. The very tough and nuanced negotiating position exposed unsupported privacy concerns.

A large hole in U.S. security was the Visa Waiver Program (VWP), which allowed European travelers, for example, to board airplanes without any data scrutiny regarding their possible terrorist affiliation until the airplane landed in the U.S. Richard Reid, the convicted "shoe bomber," used this opportunity to board a trans-Atlantic flight undetected. A new security plan was required. The objective was to find out who was coming to the U.S. and who should not be allowed to come. Each round of negotiation resulted in the E.C. retreating and raising additional points. Another adversary arose: the U.S. Department of Justice agreed to share data with other countries, but wanted to prevent DHS from doing the same because of turf jealousy. After many rounds of negotiation, the DHS was able to use advanced technology to screen an average of 400,000 arrivals each week.

The Christmas Day 2009 "underwear" Nigerian bomber demonstrates the gaps in deterring acts of terrorism. British MI5 had information about the "underwear bomber," but they did not share this with DHS because he was deemed to be a radical, rather than a potential terrorist. His father expressed his concern to U.S. Consular officials and CIA officers without avail.

Mr. Baker identifies additional and immediate future trends such as bioterrorism, international wire transfers, and financial network intrusion, and how available contemporary technology can be rapidly adapted and used by computer hackers, including computer-savvy terrorists. However, his principal nemesis is the U.S. privacy and civil liberties establishment which has gained and retained the upper hand over DHS security-related data collection projects.

Mr. Baker provides cogent and important reasons to collect and collate data for widely differing purposes so that patterns of terrorists and terrorism emerge. His counter to reasonable privacy concerns is the use of government-enforced electronic sanctions to prevent inappropriate access to data and to verify accountability. The concluding two chapters of the book are an elegant and persuasive argument regarding "what's wrong with privacy?" This essay, which is grounded on the author's unique experience, critical analysis, common sense, and balanced discernment of the American Ethos, provides a basis for informed discussion that could result in melding legitimate civil liberties concerns with the data collection component of national security.