BOOK REVIEW

A Knowledgeable Insider Warns of the Challenges in Shaping Counterterrorism Policies

SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM. By Stewart A. Baker. Hoover Institution Press, 2010. Pp xi, 370. $19.95

Reviewed by John H. Shenefield*

Stewart Baker has written an enthralling, yet alarming, account of the difficult road we as country have traveled since 9/11.[1] Part memoir of a veteran senior government official, part lesson in interdepartmental infighting and bureaucratic power games, part philosophical musing on technology's benefits and potential costs, and part vigorous advocacy enlivened by saucy humor and snappy prose, Baker's book summons us to think hard about how new technologies – air travel, computer functionality, biotechnology – jeopardize our lives and our way of life even as they also promise to brighten our futures. Standing athwart history and denying society – and its government – the right of access to technology's huge payoffs will not do and can never be successful in the long run. Baker argues, therefore, that a privacy policy that tries to lock down technology makes no sense. It would be far better to acknowledge that new technologies will over time become accessible to all, and to allow the government under strict rules of accountability to use technology to create protective systems to prevent, or blunt, horrific terrorist attacks in the American homeland.

Baker has studied these issues close up from a unique perspective. He is a recent example of the hallowed Washington institution of the "revolving door," and is one of the best demonstrations of that institution's efficacy. His prosperous big-firm law practice has regularly been punctuated by important stints in public service, much to the nation's benefit. He served as general counsel of the National Security Agency from 1992 to 1994, and then as general counsel of the Robb-Silberman Commission investigating intelligence failures in the run-up to the Iraq invasion. Most recently, he was the first assistant secretary for policy at the Department of Homeland Security from 2005 to 2009, where he grappled first-hand with the impact of technology on national security and privacy

* Adjunct Fellow, Hudson Institute; Associate Attorney General (1979-1981) and Assistant Attorney General (Antitrust) (1977-1979), U.S. Department of Justice.

1. STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010).

policies and the balance between these values. Now back in the private sector, Baker in this book reflects on all that he has just seen and experienced, laying out the lessons he has learned for the edification of his fellow countrymen.

Tellingly, the book opens with a moving account of Baker's personal pilgrimage on a rainy afternoon just after the Bush administration had left office to the memorial for those who died at the Pentagon on 9/11. He stands in the rain, musing about his struggles – some successful, some unsuccessful – to improve border and homeland security, frequently against the stubborn opposition of industry, foreign governments, and especially civil liberties groups and privacy advocates. He remembers how he had supported the creation of the "wall"[2] between law enforcement and intelligence before he left his NSA post in the mid-1990s. Although believing that the civil liberties dangers that the "wall" was supposed to prevent were exaggerated, he saw no great harm in the proposal, which was widely popular, especially among privacy advocates inside the Beltway. But all that changed on 9/11 when "the world outside the Beltway broke through, just a few yards from where [he was] standing."[3] Baker reflects:

> I'd chosen not to fight these entrenched interests in the 1990s. When I left the National Security Agency I'd written a long article that endorsed a wall between spies and cops. I've spent years undoing that mistake.
>
> Now I am leaving government again, and writing again – and hoping to keep others from making the same mistake.
>
> Call it a gift of memory.[4]

Baker's purpose in the book is to highlight the great evil that certain powerful and very popular technologies could cause if they fall into the wrong hands. To ward off such a calamity, he recommends that the government make itself smart enough to take sensible steps to defend the public. But in Baker's world certain groups are almost reflexively opposed to many of these steps. First, there is private industry with its sharp eye for avoiding additional costs to the bottom line. Then there is the opposition of certain foreign governments, often suspicious of U.S. government actions, particularly those taken as counter-terror measures. But the primary villains of the piece are privacy advocates, whose single-minded and – in Baker's mind – short-sighted pursuit of privacy protection threatens to

---

2. *See id.* at 5 ("With a wall . . . criminal investigators from agencies like the Federal Bureau of Investigation (FBI) would be forced to observe the legal restrictions that went with criminal investigative tools. They wouldn't be tempted to take the shortcut of using intelligence that had been gathered [by the National Security Agency] with less attention to civil liberties.").

3. *Id.* at 6.

4. *Id.* at 10.

make government stupid and incapable of preventing terrible danger to U.S. citizens. Baker believes that such short-sightedness cost thousands of lives on 9/11 and will do so again if allowed to prevail.

After Baker joined then-Secretary Michael Chertoff at the Department of Homeland Security (DHS) in 2005, he came to believe that 9/11 had been caused as much by technological change as by evil men. His conclusion is that long-term trends in technological development – like jet travel – could teach us a lot about lethal dangers to the homeland that need urgent attention before they got out of hand.

Certain technologies give human beings a power and freedom that are liberating. The process of exponential technological growth is "like skating on stilts that get a little longer each year" – hence the book's title.[5] With the passage of time, as the tools available to us get faster and more powerful, we're also a little more at risk. This is because technologies that enrich the lives of the average American also empower Osama bin Laden or the Unabomber Ted Kaczynski. This potential for great evil is inherent in access to the technology from the start. Baker contends that if only we had the imagination to see the danger, we would be able to prevent it. And so Baker asks: where else is our imagination failing us? Two new technologies seem to be prime candidates for urgent study and action: computer technology and bioengineering.

But first he takes the reader through the painful lead-up to 9/11. Baker catalogs the exponential growth of the international airline industry – 28 billion kilometers of air travel in 1950 had grown to three trillion by 2000. The result was that gradually – and inevitably – a revolution in border control took place. No longer were the old security measures adequate. The Visa Waiver Program, introduced in 1986, had steadily expanded so that by 2001 more than a million visitors a month were coming to the United States without visas. Any pretence to even modest vetting had been abandoned. Thirty seconds at immigration control was the outside limit for each arriving passenger, perhaps even less at JFK, Dulles, or other busy airports.

Baker then asks, logically, why an alternative was not developed so that the thirty-second arrival interview was not the last and only line of defense. Why, for instance, could information on each passenger not be gathered in advance, perhaps while the plane was still in the air? Immigration authorities, armed with such information could then decide who should be pulled aside for secondary screening. But that would require information not just from the passengers, but from across the U.S. government and from other governments as well. In short, what was needed was more and better information, and it was all needed sooner.

---

5. *Id*. at 17.

One last step was required to deal with those who attempt to defeat the system by changing identities. It would be necessary to strengthen the security standards for passports and require fingerprint records so that terrorists could not use multiple passports to enter the United States.

It all seemed so obvious once one thought about it, says Baker, but he recounts a fierce struggle to achieve even modest gains in border security against opposition to change. Proposals to give the government more timely access to sensitive information were especially controversial. Opposition came from businesses whose profit margins depended on the status quo, the privacy lobby representing both the left and the right of the political spectrum, and the international community. Baker is proud that DHS was eventually able to make revolutionary progress in securing the borders after a lengthy struggle both within the U.S. government and with those outside it.

But despite the deaths of three thousand human beings on 9/11, the opposition to revamped border security procedures very nearly prevailed. The question Baker poses starkly throughout his book is whether we can learn lessons from the border protection struggle, and apply various carefully thought-out procedures to secure other technologies such as information networks and biotechnology, and thus avoid catastrophes far worse than 9/11. He concludes that he's not at all sure that we can.

Persuading the different agencies of government first to gather and second to share sensitive information is one of the hardest nuts to crack. The story of the construction of the "wall" between law enforcement and intelligence investigators in the world of electronic surveillance – with law enforcement highly regulated by the courts and intelligence investigators less so – is now sadly familiar, but Baker tells it well and with some provocative commentary thrown in. He describes in some detail the blurring of the dividing line. For example, there is the notorious episode involving the prosecution of Soviet spy Aldrich Ames. When prosecutors received evidence derived from an intelligence investigation physical search without benefit of a court warrant, their case became vulnerable and potentially embarrassing. They quickly settled for a plea bargain, approved by the attorney general, for a sentence short of the death penalty.

The whole shambolic experience had almost been a disaster for the Department of Justice, and as a result created a renewed determination to keep the prosecutors and the intelligence investigators apart. For its part, the Foreign Intelligence Surveillance Court (FISC), already feeling defensive in the face of accusations that it was a rubber stamp supinely carrying out the will of the executive branch, was determined to provide strong protection to civil liberties. It had a powerful ally deep in the bowels of the Justice Department, the Office of Intelligence Policy and Review (OIPR), which was the liaison and gatekeeper between the intelligence investigators and the FISC. In the wake of the Ames case, OIPR tried to harden the informal wall, and thus there ensued a series of struggles between Main Justice, OIPR, prosecutors in the Southern District of New

York, and the FBI. As Baker characterizes it, OIPR seemed gradually to be losing the bureaucratic struggle when the FISC staged a coup.

If Justice lacked the heft to enforce the wall guidelines, perhaps the FISC could supply the muscle by simply turning department policy into court-ordered rules that would be imposed on any intelligence surveillance approved by the court. The wall evolved from a matter of policy to an object of law. The FISC was determined to enforce it strictly.

On several different occasions, the court discovered that the wall had failed to do its job because of what the court perceived as FBI misconduct. False affidavits seemed to have been filed in several instances; investigations were ordered; and in one case an FBI agent was prohibited from presenting any further affidavits to the court – ever – well nigh a career-ending sanction. The court had intended to send a message to the FBI and the prosecutors: there are rules, so obey them or suffer the consequences. The "wall" was the law, and the law meant what it said.

At the end of August 2001, word came that a major al Qaeda operative had entered the country. Since the tip had come from the intelligence community, only the intelligence investigators at the FBI could address it. Notwithstanding the urgency of the information, FBI lawyers who insisted that the wall be strictly maintained thwarted attempts to bring in the much greater resources of criminal investigators. As Baker says, the under-resourced intelligence investigators, without any assistance from the rest of the Bureau, were still looking for the al Qaeda operative when "September 11 dawned, bright and crisp."[6]

But that wasn't all. Baker argues that had the FBI been able to gain access to data in the airline reservation system, as many as eleven out of the nineteen hijackers could have been located. It was possible, according to Baker, that a twelfth hijacker could have been found through access to an INS watch list for expired visas, and that even the remaining seven could have been turned up by matching addresses and following obvious investigative leads.

And here we come to the essence of Baker's take-away from 9/11, the text that forms the basis for the book's main argument:

> It's foolish to write rules for government to protect against hypothetical civil liberties or privacy abuses, and even more foolish to enforce those rules as though they matter more than the security mission.
>
> I grew deeply skeptical of efforts to write new privacy limits on government in the absence of demonstrated abuses that required

6. *Id.* at 69.

> new limits. We should not again put American lives at risk for the sake of some speculative gain in civil liberties.[7]

Of course, Baker would certainly admit that this formulation is somewhat simplistic. How much "risk," how "hypothetical," and how "speculative" are questions the reader is entitled to ask. Those very questions confront policy-makers head-on whenever the most difficult national security questions arise. How much of our civil liberties must we put at risk to protect our national security, and is there a presumptive answer in the closest cases? Baker would contend that while there may be measures to protect against avoidable civil liberties abuses, those precautions should not deny the government timely access to information where denial has a plausible national security cost. Baker is unwilling to indulge in the fatuous observation that security can be protected without sacrificing any civil liberties – a familiar "mother-and-apple pie" line that never fails to evoke applause in certain circles. In the real world, he would point out, difficult choices have to be made – sometimes very quickly, often with incomplete information, never with metaphysical certainty – every day.

Most of the narrative is taken up with accounts and anecdotes about the choices that were presented to the government, and to him, in his most recent tour. They vary from the ludicrous to the terrifying. An example of the first was what Baker describes as an immense outcry when police at Logan Airport in Boston were given hand-held computers. Police use of the devices was then hyperbolically characterized by the executive director of the Massachusetts ACLU chapter as "'mass scrutiny of the lives and activities of innocent people,' and 'a violation of the core democratic principle that the government should not be permitted to violate a person's privacy, unless it has reason to believe that he or she is involved in wrongdoing.'"[8] But Baker points out that the handheld computers were linked only to public databases which any private citizen could search. Perhaps indulging in a bit of hyperbole himself, he wryly observes that "the ACLU seemed to think law enforcement should live in 1950 forever" and that "we'd better not tell them we also have access to the White Pages."[9]

At the other end of the spectrum is his assessment of the national security implications of "synthetic biology." Put simply, Baker estimates that the chance that the world will continue to remain free of the scourge of smallpox – which had been erased from nature by systematic vaccinations – is close to zero. Such is the exponential improvement of biotechnology that "[w]ithin ten years, any competent biologist with a good lab and up-to-date

---

7. *Id.* at 72.
8. *Id.* at 27.
9. *Id.* at 28.

DNA synthesis skills will be able to recreate the smallpox virus from scratch."[10]

Baker believes that inevitably this technology, like others that have become democratized, will fall into everyone's hands, and therefore ultimately into the wrong hands. The result is that millions of people will be able to feed the virus into the air of a large city populated by young and old, most no longer immunized against the threat.

How can the threat be defeated or at least minimized? First, Baker suggests, by such countermeasures as making vaccines, antibiotics, and other treatments available now so that they could be in every citizen's medicine cabinet ready for emergency use the minute an attack is discovered. A second active defense is to closely follow who actually has access to such dangerous pathogens inside the United States. Both strategies were launched after the 2001 anthrax attacks, but they have since languished.

One of the culprits is government lethargy. Baker reports that some scientists at the National Institutes of Health opposed the program because it meant loss of funding for their own research projects. The Department of Health and Human Services (HHS) has been reluctant to put in place realistic regulations for approval of counter-measure drugs, and thus they remain unavailable to the general public. Speed in treatment will be essential; hours will be crucial and days decisive in limiting the scale of the disaster. Baker tells us that following an anthrax attack, almost all of the targeted population would survive if treated within three days. On the other hand, half might not survive if they had to await treatment for five or six days,

But what is the current plan to deliver antibiotics to the population? Baker says that delivery depends on the U.S. Postal Service. Baker sets out in excruciating detail the logistical nightmare that such a plan entails, including the difficulty of providing security to the postmen, getting routes straight, protecting the mailboxes containing antibiotics from thieves or even those who are dying for lack of medicine. And how likely is it, he asks, that a heavily unionized postal service would easily and quickly agree to show up for work and drive into anthrax-contaminated neighborhoods to distribute antibiotics? Five or six days begins to seem like an impossibly short time.

The second prong of an active defense – finding out who has access to the biotechnology tools to create deadly viruses – likewise has foundered on the rocks of bureaucratic refusals and privacy lobby objections. After the 2001 anthrax attack that killed seven people, Congress adopted a registration-and-accountability program that would make background checks possible for researchers who work with biological agents. DHS

10. *Id*. at 277.

suggested that the database be digitized so that it could be easily updated and quickly accessed. Baker reports that the FBI and HHS resisted suggestions for improvement, and HHS adamantly refused to supply to DHS the data already collected. Unsurprisingly, privacy grounds were asserted as the reasons for refusal, conveniently reinforcing the natural bureaucratic instinct to hold information close. For the moment at least, the defense against unleashing synthetic smallpox had been taken off the field.

Baker concedes that some modest progress has been made since he left public office, but far less than is required. The measure that would most effectively work to achieve biosecurity is a legislated safety standard required for biotech companies in order to get patent protection. But Baker sees that requirement as running into a buzz saw of hostility from "business, privacy, and international interests, and that's why it probably won't happen, at least not until the ever-steepening curve of biotechnology produces a disaster."[11]

Cybersecurity is another entry in the Baker catalog of disasters waiting to happen. He recites the history of cyber crime and cyber attacks, from hacking for fun and criminal spam, through "distributed" denial of service attacks, malware breaches of financial and military systems, identity theft on the social media, and illicit control of computers and networks by foreign nations and organized crime. Computers that have been compromised can become "zombies," then act as "botnets," responding to the commands of remote controllers, usually without the knowledge of the computers' owners or operators.

In 2007, large-scale cyber attacks were perpetrated against Estonian federal government and banking systems, perhaps the work of the Russian government. In 2008, Russia attacked Georgian websites. Systems carrying sensitive data are not free from attack simply because they are separated from the Internet by an "air gap."[12] Both French and British air forces have been grounded after penetration by the "Conficker" computer worm. And Baker points out that attacks on U.S. systems tend to be hydra-headed, first stealing secrets, then corrupting back-up files, and finally bringing an entire system down. If an attacker changes data and emails, the system may soon become completely untrustworthy.

Can the U.S. government take even modest steps to counter these threats? Baker cautions that the defensive path is a difficult one. For instance, the federal government has proposed implementation of intrusion detection systems for federal networks that would enable the government to read its own mail and inspect it for malicious software. But civil liberties advocates have strongly opposed such systems, and Baker fears that such

11. *Id.* at 305.

12. An "air gap" is an ultra-secure network security scheme where high security networks are isolated completely from any connection to a less secure system.

resistance may ultimately prevent their adoption. Already, opposition has caused ten years of delay.

Baker suspects that the best way to achieve cybersecurity might be to construct a wholly new architecture with accountability that runs alongside – but separated from – the old anonymous Internet. That would solve the attribution problem, which today prevents identification of cyber attackers who hop from computer to computer and from country to country. Baker correctly predicts that if loss of anonymity were ever proposed for the conventional Internet, privacy advocates would cause a meltdown. But are there measures short of a new system that might work? Just prior to the end of the Bush administration, DHS drafted a report suggesting various incentives and regulations. It went nowhere, and Baker observes that not much has happened since, notwithstanding the fact that candidate Obama – whose campaign network had been systematically penetrated and exploited by foreign intelligence operators – pledged that cybersecurity would be a top national security priority. Once again, privacy and business interests prevailed.

At the very end of the book, Baker zeroes in on a pivotal policy question that has nagged him since 9/11:

> But why are privacy groups so viscerally opposed to government action that could reduce the risks posed by these exponential technologies? . . . [I]n the fields where disaster has not yet struck – computer security and biotechnology – privacy groups have blocked the government from taking even modest steps to head off danger.[13]

Baker begins with the venerable 1890 Harvard Law Review article[14] in which Louis Brandeis and his law partner Samuel Warren, reacting to unwanted press coverage of a social event, set about creating the new right of privacy. Baker finds the article thoroughly anachronistic – "laughable" – even though it is still cited reverently by privacy advocates. According to Baker, the spirit of the article, its firm support of the status quo, lives on in the privacy activism of today, particularly in the effort to stop government from using new technology to harness information for the public good. He argues persuasively that opposing technological change is not a winning strategy, particularly when the cost of making government less effective can be reckoned in numbers of lives lost.

So what is Baker's answer to resolving the tension between information technology and legitimate privacy interests? Of course we should protect privacy, but not by depriving government access to technology's benefits.

---

13. Baker, *supra* note 1, at 309.

14. Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Thus he rejects privacy protection efforts that rely on the notions that: 1) personal data is private property; 2) access to personal data should require a legal predicate; and 3) government should comply with limits on the use of personal data. The first is ineffectual to protect privacy and has large social costs – creativity is stifled and free speech muzzled. The second is also ineffectual, and can have immensely harmful consequences, such as allowing potential terrorists to litigate every data seizure, and therefore some inevitably to go free. The third limits needed government flexibility and results in the paradox that government may have information for one purpose that it cannot use for another more important, yet unforeseen purpose.

What *will* work? Baker's answer is electronically enforced accountability. Do not prevent the government from having access to data, but punish government for any misuse. If candidate Obama's passport file is searched for improper reasons, find out who crossed the line and punish the wrong-doer. If Joe "the Plumber" Wurzelbacher's celebrity in the 2008 campaign results in eighteen separate breaches of his personal data, trace the intruders and punish them. Baker points out that network security and audit tools now available make it easy to enforce usage rules. That, as he says, is "a privacy policy that could work. And a technology policy that makes sense."[15]

In sum, this is a thought-provoking book that will irritate some, and cause others to lose sleep. It is filled with fascinating anecdotes, unusual insights into the policymaking machinery, both in Washington and in Brussels, and introduces fresh and politically incorrect ideas about some of the household gods enshrined in our nation's political ideals.

But Baker's argument is crisply presented, and his supporting evidence is impressively arrayed. Those on the opposite side of the policy debate must confront his conclusions. Here is a candid addition to the conversation about national security. We ignore it at our nation's peril.

15. Baker, *supra* note 1, at 341.