The Open Society Paradox:
Why the Twenty-First Century
Calls for More Openness, Not Less

Dennis Bailey
mail@dennisbailey.com

March 2004

Part I: The Enemies of Open Society

Chapter 1 – Introduction – The Devil Has A Deal for You!

When you're in the outer world, you have to act like them, dress like them, behave like them.— Quote from an al Qaeda handbook mentioned in East Kenyan Embassy bombing trial[i]

In November 1999, when Khalid al-Mihdhar and Nawaf al-Hamzi moved into the Parkwood Apartments in San Diego's Clairmont District in California, they appeared to be two ordinary Muslims trying their best to fit in and stake their claim to the American dream. A local Islamic center helped them settle into the community and afforded them the opportunity to practice their daily religious routines. They enrolled in aviation lessons at Sorbi Flying Club near Montgomery Field, a small San Diego airport, something foreign nationals occasionally did in an attempt to parlay quality U.S. training into well-paying jobs in their home country. They played soccer in the park, ate fast food, had season passes to Seaworld, even frequented a strip club—essentially nothing that would suggest that they were anything other than two average foreigners trying to make it in the world.

A few things were peculiar about al-Mihdhar and al-Hamzi, however. According to reports, neighbors wondered why they would use their cell phones outside the house whenever they had to make a call. Perhaps it was because they had barely any furniture in their house. With few furnishings, the two would eat their meals on the floor. They'd also play flight simulator games for hours, which neighbors observed through the frequently open front door. Most strange of all was that even though the two men apparently couldn't afford to buy furniture, they were often picked up in fancy limousines with tinted windows.

Despite these few quirks, there is little reason to think that two people as seemingly innocuous as al-Mihdhar and al-Hamzi would raise suspicion among Americans accustomed to the idiosyncratic behavior showcased daily in a parade of reality shows and supermarket tabloids. The FBI, which had a long-time counterterrorism informant in contact with the two men, didn't appear to be concerned. Apparently the Central Intelligence Agency (CIA) wasn't overly worried either, even after receiving information from Malaysian intelligence that the two had visited with al Qaeda operatives in Kuala Lumpur in January 2000. It wasn't until August of 2001 that the CIA finally raised the alarm and urged the Federal Bureau of Investigation (FBI) to locate the two men. By then it was too late. Al-Mihdhar and al-Hamzi had successfully disappeared into American society in preparation for their mission.

On September 11, 2001, when al-Mihdhar and al-Hamzi helped hijack American Airlines Flight 77, the U.S. government and residents of San Diego's Clairmont District finally began to

realize that these apparently ordinary men were part of a larger group of al Qaeda militants determined to commit atrocities against the United States. In a post–9/11 world, where Americans are under threat of additional terrorist attacks, the tragic success of al-Mihdhar, al-Hamzi, and the other hijackers forces us to ask a fundamental question: How do we protect an open society from those who would use its freedoms against us?

Many who have reflected on 9/11 suggest that the attacks were a watershed event, signaling the changing nature of threats that challenge the United States. During the Cold War, anxiety was somewhat alleviated by knowing who the enemy was and by knowing that this enemy was, in fact, oceans away. Today that guarded sense of security has morphed into unease over a faceless enemy that lives in American neighborhoods and is dedicated to jihad against the West. The U.S. military, designed to face more traditional challenges such as chasing Saddam Hussein out of Baghdad or keeping North Korea on its side of the 38th parallel, appears to be ill-equipped to counter the shadowy and decentralized enemy in this first war of the twenty-first century. Chapter Two begins an exploration of this brave new world by looking at modern madmen who seek to overthrow the West through an ideology that distorts the teachings of Islam.

Overlooked in discussions on the war against terrorism is the distinguishing characteristic that made America vulnerable to the likes of al-Mihdhar and al-Hamzi in the first place—its openness. We typically think of an open society as the crowning achievement of man. Free markets, human rights, the free exchange of ideas and information, and representative government—these principles of Democracy have brought unparalleled wealth, prosperity, and freedom to U.S. citizens and all but vanquished twentieth-century competitors such as Fascism and Communism.

Yet 9/11 reminded the world that the openness and freedom valued in Western democracies could be exploited for malevolent purposes. Citizens from Northern Ireland or Israel, who themselves have faced lunatics armed with bombs for decades, know all too well about the susceptibility of open societies to violence.

The United States, the freest and most open of all democracies, must have been a particularly inviting target to a fanatic like Osama bin Laden. With America's porous borders, ease of mobility and communication, and relative anonymity, al Qaeda's leaders knew they could train their terrorist operatives to infiltrate the country and assault any number of targets. Armed with driver's licenses, social security numbers, bank accounts, and cell phones, the terrorists had the freedom to coordinate the 9/11 attacks knowing that their activities would blur anonymously into the noise of millions of other Americans going about their daily lives. This idea, that

terrorists could pervert a cherished value like anonymity into a weapon, prompts the discussion that begins in Chapter Three. The chapter suggests that while a little anonymity is a good thing, untraceable anonymity particularly the kind that is developing on the Internet is giving the likes of copyright violators, spammers, traffickers in child pornography, hackers and worst of all─ terrorists─ the ability to roam the digital world with free reign. Chapter Four continues the debate on anonymity by using the growing problem of identity theft to illustrate the risks society faces when individuals are able to shield their identities to escape accountability. The chapter asks the provocative question of whether identity theft is more of a security rather than a privacy issue and it surmises that a majority of our worst fears over personal data and privacy would melt away if identity theft could be eliminated.

The risks inherent to open societies were discussed long before 9/11. The conventional wisdom has always been that a free country like the United States has to allow for a certain amount of lawlessness and violence knowing that the only other alternative is a police state, one that could effectively stamp out crime but at the price of our freedom. William Safire of the *New York Times* encapsulates this idea: "When Patty Hearst managed to remain a fugitive for 591 days, that did not mean the FBI was bad at catching fugitives; it meant that America was a free society. In China or the Soviet Union, she would have been captured in days, because it is impossible for ordinary citizens to move about without permission. If our values mean anything at all, they mean that it is better to tolerate the illegal movement of aliens and even criminals than to tolerate the constant surveillance of the free."[ii]

The question of finding the right balance between security and freedom can be traced back to the Founding Fathers who struggled to form a government that would provide for the safety and common defense of Americans without leaving too much power in the hands of the state. The Federalist Papers sum up this dilemma succinctly: "In framing a government which is to be administered by men over men, the greatest difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[iii]

Although discussions of how to best create a government that represents the people and protects their natural rights dominate the Federalist Papers, the question of security is never far from the minds of the authors. They understood that the informal contract on which society is based provides a guarantee of safety and welfare for the public that is not found in the state of nature. John Locke, the seventeenth-century philosopher who greatly influenced the Founding Fathers, said the following in his "Second Treatise on Civil Government": "In all states of created beings, capable of laws, where there is no law there is no freedom. For liberty is to be free from

the restraint and violence from others; which cannot be where there is no law; and is not, as we are told, a liberty for every man to do what he lists."[iv]

The question of ensuring security within a free society has been made relevant once again by recognition of the state of the world following September 11. The Faustian bargain of trading security for the alluring promise of freedom may have seemed reasonable when the only downside was tolerating the occasional robbery or mugging in a mostly civil society. But in the age where a deranged lunatic might obtain weapons that confer a godlike power of destruction once reserved for superpowers, ignoring the founder's lessons that men cannot be free unless they are first secure may see us on the losing end of a deal with the Devil.

This book argues that technology is creating a world where we may not be forced to choose between freedom and security. New tools of openness that inject transparency into public life are available that can help identify fanatics like al-Mihdhar and al-Hamzi, while allowing average Americans and foreign visitors to go about their lives without interruption.

Part II of this book, starting with Chapter Five, explores recent developments in secure IDs and biometrics, two technologies that can identify terrorists at U.S. borders or prevent them from changing identities if they do manage to enter the country. This chapter bravely argues that the current paper-based system of identification is undermining practically all of the government's efforts in the war against terror.

Chapter Six investigates surveillance technology such as facial recognition that can uncover terrorists if they appear at secure sites such as airports or government buildings. It concludes by asking whether cameras that recognize faces are really any different from small town communities where most residents are recognized on the street.

Chapter Seven examines information analysis, the third component in an arsenal of openness and a technology that refers to intelligent computer programs that can pick through mundane electronic records to find meaningful clues that terrorists leave behind. Congressional investigators since 9/11 have consistently lamented the failure of intelligence agencies to share information; unfortunately these same investigators have wilted in face of the rhetoric of "Big Brother" and other attacks on programs like Terrorism Information Awareness (TIA) that were intended to solve the information sharing problem.

Taken together, Chapters Five through Seven paint of picture of new technologies which when used together can remove the camouflage of anonymity that terrorists find in open societies, making them stand out from the crowd in bas-relief.

Although these technologies are useful in the anti-terror campaign, when used appropriately, they can respect civil liberties at the same time. In fact, one surprising idea discussed in this book is that whenever there is an increase in transparency, there may be a corresponding rise in the freedom and mobility that most Americans expect. More openness has the effect of reducing the burdens of security, for example, facilitating the boarding of airplanes for "trusted" American travelers by eliminating the need for an invasive search or intensive interrogation. It's only when authorities have limited information about real threats that they are forced to treat everyone like a suspect or focus on factors such as ethnicity or religion that have poor validity as predictors of terrorism and create resentment among people. At the same time, transparency ensures that if an airport official mistreats someone or violates his or her rights, the injustice does not go unnoticed.

What these technological advances suggest is the open society paradox. Although it was openness that left the United States vulnerable to the heinous intentions of radicals on 9/11, it is more openness, especially when it pertains to information, which serves as the country's greatest defense. With technologies that facilitate greater transparency, a would-be terrorist raising money or finding recruits for a planned attack will now have to worry that his source of funds will be electronically traced, his ties to other terrorists uncovered through computer analysis of Internet or cell phone patterns, or that his fingerprints or photo linked to an international database of terrorist suspects.

This suggests that the answer to twenty-first century threats is not to close society by putting more police on the streets, shutting down its borders or constructing walls of privacy around its citizens; paradoxically, it is the opening of society that exposes the shadows where terrorists lurk.

The acceptance of more transparency is not a fait accompli for most Americans. If scrutiny can be used to expose terrorists living among us, we must consider that it may also expose aspects of our own lives. For many Americans concerned that greater watchfulness will reveal personal details of their lives, a policy of openness may need to be reconciled with the country's longstanding desire for privacy.

Part III of this book takes a step in that direction by arguing that a twenty-first century approach to an open society requires a reconceptualization of privacy. Chapter Eight, for instance, challenges the romanticized view that there was once a "Garden of Eden" of privacy to which we should seek to return. Many readers might be surprised to learn that privacy as it is now conceived is a relatively modern development.

Chapter Nine counters the notion that privacy is an absolute right akin to liberty and therefore should never be limited, even in matters of national security. The chapter opines that even if someone's privacy is limited, it rarely restricts their freedom and when it does, there is usually legal recourse.

Chapter Ten tries to separate fact from fiction by questioning the idea of government as a Big Brother that seeks to destroy our most cherished liberties. In an unexpected defense of the U.S. federal government, the chapter uses events from the Watergate scandal to the *USA PATRIOT Act* to argue that the Founding Father's system of checks and balances has served democracy as intended.

Chapter Eleven debunks myths about another privacy bogeyman, corporate America, arguing that restrictions on information would have economic consequences and be an abridgement of a company's free speech rights. Yet before the reader concludes that the author has left consumers helpless in face of the prowess of the corporate marketing juggernaut, the chapter takes an unexpected turn arguing that an opt-in approach applied to all forms of direct marketing would cordon off some personal space for consumers. Just because a corporation has your personal information, it doesn't give them the right to harass you with email or calls to your home. As personal information continues to spread and direct marketing through digital means becomes a global affair, the need to protect consumers from the onslaught will only increase.

Chapter Twelve draws the conclusion that in a world flooded with data, we should be less focused on trying to secure personal information and more on making sure it isn't used to restrict our most basic constitutional rights. What is most critical is not whether Attorney General John Ashcroft knows that I like to travel to Europe or that I prefer to listen to Bach (privacy), but whether he restricts my right to do so in the first place (private choice). It's this conflation of privacy with private choice that causes unnecessary hand-wringing in the media on issues such as identification, surveillance and information analysis and distracts us from the essential question of whether our freedoms are truly being threatened.

Taken as a whole, these chapters suggest that it will be a more limited view of privacy based on the solid foundation of the Fourth Amendment and paired with a vigorous protection of private choice that will give us the best chance of carving out personal space and safeguarding constitutional freedoms within the realities of a century where "information longs to be free."

Will America be willing to accomodate greater openness? Notwithstanding the barrage of media stories and the harangues by civil liberty groups decrying a loss of privacy, a great many Americans have learned to accept and in many cases embrace the increasing amount of

transparency found in many aspects of their lives. Twenty-four-hour news networks and their relentless armies of reporters swarm on every scent of a story. A proliferation of surveillance cameras, continually decreasing in size, dots the urban landscape. Several C-SPAN channels cover every move elected officials make. Reality television draws millions of viewers into the private lives of ordinary Americans.

These days, there may be more readiness to hand over personal data and reveal public actions than at any time in recent history. Consumers numbering in the millions use grocery shopping cards to receive discounts on purchases. A growing number of working parents monitor daycare centers from the office. Online shoppers willingly hand over credit card numbers to complete Internet transactions at the click of a mouse. In many ways, the public has come to acknowledge what the courts have ruled for years: there is little reasonable expectation of privacy in our public lives.

Nevertheless, many skeptical Americans know that an apparatus of openness in the hands of the government offers great temptation for abuse. They have a right to be concerned after witnessing the many perversions of power in the last century. They've watched as the FBI spied on Americans and infiltrated activist groups. They've seen a total disregard for authority by a president during the Watergate scandal. They've read countless history books documenting the scandals, corruption, and threats to liberty experienced in this country since its inception.

Chapter Thirteen suggests that if the public is to embrace greater openness, they will expect the same from their leaders. Unfortunately, while the U.S. government is pushing for enhanced powers to battle foes like al Qaeda, they are resisting the implementation of transparency measures that would expose their own actions. The Bush administration has been particularly culpable in cultivating a culture of secrecy in everything from resisting *Freedom of Information Act* (FOIA) requests to planning enhancements to the *USA PATRIOT Act* without consulting Congress. An asymmetrical transparency, which allows the government to watch over the people and not vice versa, is a historical design for disaster.

It may be that there are forces at work driving us toward more transparency that even the U.S. government and other leaders around the world will not be able to resist. The drive for efficiency and the thirst for information in modern societies, undergirded by the exponential growth in technology, will leave little cover for leaders who misuse their authority behind closed doors. For most Americans, a revitalization of trust and accountability will restore the principle of reputation that was once the basis for relations in the village, making it possible to improve collective judgments of who can be expected to act in accordance with societal obligations. And

as for the al-Mihdhars and al-Hamzis of the world who seek our destruction? They will be affected the most as they discover that a career in terrorism has become a dead-end job.

---

[i] Johanna Mcgeary and David Van Biema, "The New Breed of Terrorist: An exclusive look at the lives of the men behind the strike. Now dozens of their associates may be at large in the U.S. What will come next?" *Time,* September 24, 2001.

[ii] Quoted by Joseph W. Eaton, *Card Carrying Americans: Privacy, Security and the National ID Debate* (New Jersey: Rowman & Littlefield, 1987), 111.

[iii] Alexander Hamilton or James Madison, "The Structure of thee of the Government Must Furnish the Proper Checks and Balances between the Different Departments," From the New York Packet.
Friday, February 8, 1788. The Federalist Papers, No. 51.

[iv] John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988), 305.