COMBATING TERRORISM IN THE DIGITAL AGE: A CLASH OF DOCTRINES: THE FRONTIER OF SOVEREIGNTY—NATIONAL SECURITY AND CITIZENSHIP—THE FOURTH AMENDMENT—TECHNOLOGY AND SHIFTING LEGAL BORDERS

Harvey Rishikof[*]

> I guarantee you this: neither the drafters of the Fourth Amendment, nor the Supreme Court when it crafted the 'border search exception,' ever dreamed that tens of thousands of Americans would cross the border every day, carrying with them the equivalent of a full library of their most personal information. . . . If you asked most Americans whether the government has the right to look through their luggage for contraband when they are returning from an overseas trip, they would tell you yes, the government has that right. But if you asked them whether the government has a right to open their laptops, read their documents and e-mails, look at their photographs, and examine the websites they have visited, all without any suspicion of wrongdoing, I think those same Americans would say that the government absolutely has no right to do that. . . . Ideally, Fourth Amendment jurisprudence would evolve to protect Americans' privacy in this once unfathomable situation. But if the courts can't offer that

[*] Professor of Law, former Chair, Department of National Security Strategy, National War College. The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the National War College, the Department of Defense, or the U.S. government.

> protection, then that responsibility falls to Congress.[1]
>
> Senator Russ Feingold 2008

> The threat of catastrophic attack with nuclear weapons has the greatest potential impact on our way of life and in terms of human cost.[2]
>
> A 2006 poll of 116 terrorism specialists representing a cross-section of political perspectives placed the likelihood of "a terrorist attack on the scale of 9/11 occurring in the United States" in the next five years (by the end of 2011) at 79 percent.[3]
>
> We are on borrowed time.[4]
>
> James E. Baker
> *In the Common Defense*

In a pre-9/11 conversation with a United States Supreme Court Justice he/she casually noted to me that when thinking about the different challenges for the law, "we are more or less settled in the Fourth Amendment area" and that the more interesting jurisprudence would be taking place elsewhere. This was a view held by many in the judicial world; however, this consensus has proven to be a premature assessment of the Fourth Amendment and the role of the Supreme Court.

Those who maintained this position underestimated the relationship of critical trends in the marketplace, the nature of modern threats to the state, theories of sovereignty and how the

---

[1] *Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. (June 25, 2008) (statement of Sen. Russ Feingold, Chairman, Subcomm. on the Constitution of the S. Comm. on the Judiciary), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=3420&wit_id=4083 (last visited Nov. 28, 2008).

[2] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 307 (Cambridge Univ. Press) (2007).

[3] *Id.* at 242.

[4] *Id.* at 6.

modern state has begun to approach the concept of privacy when it comes to borders. In fact, these new threats to the state, given the context of the law, have made "border security" and our understanding of the Fourth Amendment, an intellectual pivot point for our expectation of privacy in the 21st century. The state, in the face of a rapidly changing world of technology and while pursuing its fundamental prerogative to defend the nation, has taken a theoretical position, supported by the Supreme Court, that is transforming our very notion of citizenship.

In order to present my argument it is necessary to begin with a set of interlocking propositions that concern the evolving market place in the digital age of communication, the nature of modern threats to the state, the authority of the state to defend itself and the current threads of Supreme Court constitutional analysis in the Fourth Amendment arena. This paper will conclude with a discussion of how these interlocking propositions have created a clash of legal, political and social doctrines.

I. A SET OF INTERLOCKING PROPOSITIONS:

A. The Market Place: The Digital Age of Communications

The technological computer revolution is not reversible. The world of laptops, cell phones, PDAs, MP3 players and memory sticks has created an information revolution. This "portability" of property and expression has created an ability to generate a sea of information, transport the sea of information and then comment and create new seas of data. The full ramifications of this revolution are still being played out as a social force.[5]

[5] The concept of "ubiquitous technology" was explored in a law journal article by Susan Brenner where she noted that the physical and informational barriers historically used to differentiate between the public and private sectors of individuals' lives were being undermined by technology, and the Fourth Amendment would require "spatial" updating to remain viable. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L. J. 1, 83 (2005).

The Internet has contributed by creating "pipes" and downlinks that allow interglobal communication from Shanghai to Washington in the blink of an eye. We all have become accustomed to the ability to communicate seamlessly at any time, from any place, with a variety of devices at our disposal.

It is believed that the next predicted revolution will take place in the soft "bio-technological" arena where billions of dollars are being invested to create products that will be able to store even greater banks of data on even smaller and more transportable devices. In fact, "chosen VIP clubbers" in Barcelona have been able to implant RFID chips in their arms that allow them to enter nightclubs with an electronic scan and pay for drinks with a similar scan.[6] The chip negates the need for identification cards or even money, since it acts as a debit card.[7] Given the technology, vast amounts of information could be similarly placed on a chip, implanted in an arm and then transported across the border. Where this type of technology will lead is limited only by the imagination.

These developments have contributed to the erosion of borders pertaining to the passage of information. The world of *hard copy* information remains only for the final act of reading; technology has already placed in the market the "electronic book tablet" that allows entire texts to be downloaded and electronically marked for underscoring and quoting.[8] This innovation potentially allows for downloading reading material at multiple access points. Moreover, as has been documented elsewhere, these technological changes have created a different

[6] Posting of Duncan Graham-Rowe to New Scientist news blog, *available at* http://www.newscientist.com/article.ns?id=dn5022 (May 21, 2004) (last visited Nov. 28, 2008) ("The chips are 1.2 millimetres wide and 12 millimetres long and look like a long grain of rice. A medically trained person injects the chip under the skin in the upper left arm, by the triceps. A scanner reads the chip by emitting a radio signal. This energizes the chip and causes it to send out a small radio frequency signal. This can be picked up from about 10 centimetres away.").

[7] *Id.*

[8] James Thompson, *The Big Question: Do electronic books threaten the future of traditional publishing?*, THE INDEPENDENT, July 24, 2008, *available at* http://www.independent.co.uk/life-style/gadgets-and-tech/features/the-big-question-do-electronic-books-threaten-the-future-of-traditional-publishing-875724.html (last visited Nov. 4, 2008).

approach to information and access for the next generation. The new generation of MySpace, Facebook and YouTube users are more open about information, share more easily and assume a reduced sphere of privacy.[9]

In short, the first proposition is that the digital information super highway is *omnipresent* and *omniaccessible* and *irreversible*. These developments have led some to question whether national borders are just speed bumps on the information super highway. How will or should the state and law respond to this proposition?

B. The Modern Threats: Individualized Privatized Weapons of Mass Destruction to Economic Espionage

The leitmotif for the twenty-first century is the increased "individualization" of the threat to the modern state. Niall Ferguson, in a book review provided that Phillip Bobbitt, the noted national security theorist, describes the terrorist threat as the intersection of "decentralized, privatized, outsourced and in some measure divorced from territorial sovereignty."[10] Individuals have access to a potential toxic cocktail of nuclear, biological, radiological and chemical weapons that can trigger mass destruction. A former special assistant to the President, legal adviser to the National Security Council, and now federal judge for the Court of Military Appeals, described "the threat of catastrophic attack with nuclear weapons" as having "the greatest potential impact on our way of life . . . in terms of

---

[9] Anthony Lilley, *Public is the new private for the MySpace generation*, THE GUARDIAN, March 23, 2006, at 8 of Media news and feature, *available at* http://www.guardian.co.uk/media/2006/mar/20/mondaymediasection.digitalmedia (last visited Nov. 28, 2008). Naturally, there is a movement to regain one's anonymity. One is the "de-tagging" phenomenon, whereby one tries to remove his or her name from a picture on Facebook; however, the picture continues to exist somewhere. *See* Lisa Gurensey, *Picture Your Name Here*, N.Y. TIMES at 6, July 27, 2008, *available at* http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html (last visited Nov. 28, 2008).

[10] Niall Ferguson, *War Plans*, N.Y. TIMES, April 13, 2009, *available at* http://www.nytimes.com/2008/04/13/books/review/Ferguson-t.html (last visited Dec. 2, 2008) (Terror and Consent book review). *See also* PHILIP BOBBITT, TERROR AND CONSENT (Alfred A. Knopf 2008).

human cost" and being a threat that is "perpetual, indefinite, endless, and not just long."[11] This is the widespread consensus among practitioners. "A 2006 poll of 116 terrorism specialists representing a cross-section of political perspectives placed the likelihood of a 'terrorist attack on the scale of 9/11 occurring in the United States' in the next five years (by the end of 2011) at 79 percent."[12]

What makes the threat so bedeviling is that it is not state based, per se. Since the Treaty of Westphalia in 1648, the unit of analysis for the international system has been the state. The advantage of the state being the source of a threat is that the sovereign is subject to deterrence. Following the Treaty, all sovereigns understood that they could be held responsible for any projections of force and that retribution might result in the personal loss of power and ultimately, subjugation of their people to a new, more powerful political entity. This "realist" perspective, based on the history of modern warfare, acted as a restraint on action until a state calculated whether it would be able to use force and not be disciplined or whether it would acquire enough force to begin a campaign of expansion and suffer the consequences if defeated. The advent of nuclear weapons has raised the stakes for this calculation since now the potential for total annihilation is a possible outcome of any reckless use of force. The modern era of mutually assured destruction between the superpowers produced at times an anxiety-ridden *Pax Americana*, but it achieved the ultimate goal of restraining nuclear use.[13]

This international system of nuclear restraint has been upset by the potential ability of a small group of fanatically dedicated individuals to acquire and explode a nuclear bomb. The technology, although far from simple, is not so difficult as to make it impossible. One merely needs the fissionable material, a triggering mechanism and a delivery system. When possessed by a state, deterrence has been the solution since a delivery

[11] BAKER, *supra* note 2, at 307, 309.

[12] BAKER, *supra* note 2, at 242.

[13] *See* HANS MORGENTHAU, POLITICS AMONG NATIONS: THE STRUGGLE FOR POWER AND PEACE (Alfred A. Knopf) (4th ed. 1967).

system is usually associated with missile capacity.

The focus on missile capacity is unfortunately a failure of imagination. From the world of fiction, a former television journalist imagined one of the more creative solutions for a "delivery system."[14] In the novel *A Murder of Crows*, the Soviet Union, in an effort to undermine the United States nuclear "missile shield" and encourage disarmament, smuggles into the country sixty thermonuclear devices disguised as large industrial boilers.[15] The plan is to pre-position the "devices" in a number of major cities, thus neutering the missile shield and undercutting any potential for a preemptive first strike by the United States.

Although there is much "urban legend" commentary about Russian suitcase bombs and terrorist groups, the more recognized fear is a "dirty bomb" or a small bomb with radiological material as a component.[16] In the real world, the assassination of the ex-KGB agent Alexander Litvinenko in the streets of London in 2006 with polonium exposure raises the unsettling conclusion that either the incident was Russian state-sponsored, or a criminal gang was able to procure extremely dangerous and toxic radioactive material for the murder.[17] In fact,

> In the opening of Graham Allison's book, *Nuclear Terrorism,* Allison describes how the Central Intelligence Agency director, George Tenet, at the Presidential Daily Intelligence Briefing on October 11, 2001, informed President Bush that he had information that Al Qaeda had acquired a stolen Russian ten-kiloton nuclear bomb and that the source of the information believed the weapon was in New York City. According to Allison, in a moment of gallows humor, a staffer quipped that

---

[14] STEVE SHEPARD, A MURDER OF CROWS (Lyford Books) (1996).

[15] *Id.*

[16] Dan Vergani, *Experts close the lid on "suitcase nukes,"* USA TODAY, Mar. 12, 2007, at 9D, *available at* http://www.usatoday.com/tech/science/2007-03-12-suitcase-nuclear-bombs_N.htm (last visited Nov. 28, 2008).

[17] *See* Thomas de Waal, *Murder Most Foul: Following a deadly polonium trail from London back to Russia*, WASH. POST, July 27, 2008, at BW03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/07/24/AR2008072402621.html (last visited Nov. 28, 2008).

> the terrorists could have wrapped the bomb in one of the bales of marijuana that are routinely smuggled into cities like New York. The report proved to be false—this time.[18]

This Allison anecdote, for the purposes of this analysis, has the advantage of linking the contraband drug trade with terrorism in the violation of borders. As has been known for a long time, drug traffickers have been extraordinarily successful in penetrating our borders. In fact, the so-called "War on Drugs" has been successful in the sense that the street price for most drugs has remained low and accessible to the average street user.

Another threat to national security involving borders, although less popular and currently less recognized, is economic or industrial espionage.[19] In the words of Bernard Esambert, a president of the Pasteur Institute, "'Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor. . . the companies are training the armies and the unemployed are the casualties.'"[20]

When viewed from the perspective of National Counterintelligence Executive (NCIX), the governmental body charged with protecting economic security, trying to protect economic secrets in a world of shifting boundaries, world supply lines and spheres of influence is a monumental challenge:

> Boundaries of every kind are eroding—legally, behaviorally, electronically—in all aspects of our lives: Between the public

---

[18] Harvey Rishikof, *Long Ward of Political Order—Sovereignty and Choice: The Fourth Amendment and the Modern Trilemma*, 15 CORNELL J.L. & PUB. POL'Y 587, 587 (2006) (citing GRAHAM ALLISON, NUCLEAR TERRORISM: THE ULTIMATE PREVENTABLE CATASTROPHE (Times Books, Henry Holt & Co. 2004)). To see the effects of a ten-kiloton nuclear bomb, *see* www.nuclearterror.org. *Id.* at 587 n.2.

[19] *See* Harvey Rishikof, *Economic or Industrial Espionage—Who Is Eating America's Lunch? How Do We Stop It?*, *in* VAULTS, MIRRORS AND MASKS: REDISCOVERING U.S. COUNTERINTELLIGENCE (edited by Jennifer E. Simms & Burton Gerber, eds., forthcoming 2008).

[20] Wanja Eric Naef, *Economic and Industrial Espionage: A Threat to Corporate America?*, INFOCON MAGAZINE, Oct. 2003, *available at* http://www.iwar.org.uk/infocon/print/espionage-cid.htm (last visited Nov. 28, 2008).

> and private behavior of ordinary people; for example, the sense of dress and decorum appropriate to the home, the street, the office, or houses of worship. Between the public and private—that is, secret—behavior of governments. Between the financing, legal norms, and research activities of public as opposed to private institutions; [and] universities, for instance. Between state and non-state actors and the relative size of the resources they control. Cyber boundaries are also eroding—and not always in ways we like—but simply because we are sometimes helpless to enforce them.[21]

But those in government positions of authority are still responsible, and they have to try to craft a response to the new era of globalization, computerization, secrets and spying. The mission therefore is increasingly difficult and will not go away because the stakes are so high. In the elegant words of Joel Brenner, director of the NCIX, the "intellectual thieves" seem to have the upper hand at the moment.[22] As he recently explained at a public-private sector conference:

> The public and private sectors are both leaking badly. I'm not talking about just the pirating of DVDs and movies in Asia. I'm talking about significant technologies that are walking out of our laboratories on electronic disks, walking onto airplanes bound for foreign ports, and re-entering the country as finished products developed by foreign entrepreneurs. In effect, we're buying back our own technology. This is bad enough when we're talking about commercial innovation. But when we're talking about technology with substantial defense applications, we're talking about losses of intellectual capital that in wartime could cost many lives or our fellow citizens. These losses are occurring, and they are occurring in a targeted, systematic manner. Protecting innovative technology before it can be patented or classified is an urgent task, and it is difficult. If any of us knew how to do it, he'd be very rich,

[21] Dr. Joel F. Brenner, Welcoming Comments by Nat'l Counterintelligence Executive Dr. Joel F. Brenner, DNI—Private Sector Workshop on Emerging Techs. at Carnegie Endowment for Int'l Peace (Dec. 7, 2006), *available at* http://www.ncix.gov/publications/speeches/CarnegieSpeech20061207.pdf (last visited Nov. 28, 2008).

[22] *Id.*

because it's a question of handicapping basic research.[23]

The second set of propositions therefore is that the new threats are individualized, multivaried, potentially lethal on a mass scale, and potentially devastatingly costly on the economic ledger for research and development and competitive advantage. There is a clear and justified need for the state to patrol the borders so that both "blood" causing damages do not enter and economic "treasure" does not leave.

C. The Weberian Theory of The State: Consent—Authoritarian or Citizen Based—But State Power Remains

There are many ways to define a state for political and legal purposes. The *Weberian* definition for the purposes of the argument is the most helpful since it defines a state in legal and physical or geographical terms—"the *monopoly of the legitimate use of physical force* within a given territory."[24] The physical or territorial aspect of the definition is significant because it grants borders a special theoretical significance for a state's power. More significantly, the concept of citizenship is not part of the *Weberian* world of state definition since it centers authority on the legitimate use of force internally. The *Weberian* approach is essential to the Westphalian world of state powers, since internal domestic issues are excluded from the definition. Regardless of the process by which the monopolization of power is "legitimized," whether by democratic consent or authoritarian performance, a physical border must bound the state's writ. Physical borders therefore, have the potential to become special *legal areas* and the sovereign has particular powers over citizens and non-citizens alike, at the moment of entry. This approach is a fundamental challenge to U.S. jurisprudence, which has created a special and sophisticated jurisprudential framework for fundamental rights protection predicated on the idea of "citizenship," in contrast to an "authority" based concept of state

[23] *Id.*

[24] MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 154 (The Free Press 1964).

power.[25]

It is well recognized in political theory and comparative politics that the sovereign has special authority to protect the homeland and its people. One needs to underscore people, not citizens, since even today viable and significant states such as Saudi Arabia continue to have subjects, rather than voters. This core right to protect internally is enshrined in the democratic doctrines of "peace order and good government" in Great Britain[26] and *raison d'etat* in France.[27] Even our own U.S. Constitution has the "suspension clause" for the writ of habeas corpus, where in particular domestic emergencies such as rebellion or invasion the "public safety may require it."[28] Despite some views that the executive branch decides when to invoke the suspension, it is clear that this right to protect rests in Article I of the Constitution though the Supreme Court retains the role of deciding what constitutes a rebellion or invasion and when the public safety requires the state to ignore the core individualized writ of habeas.[29] Under the U.S. Constitution and the *Weberian* school of state power, it is an attack on the monopolization of power in the form of a rebellion or invasion which triggers the authoritative power of the state to trump the citizenship or individualized right of habeas. To be sure, under the U.S. Constitution, it is Congress (the institution most representative of the Madisonian factionalized interests) that makes the determination and not one individual as embodied in the office of the President; further, it is assumed that the suspension will be temporary or until public safety and

[25] *See* JOHN WILLIAM SALMOND, JURISPRUDENCE OR THE THEORY OF THE LAW 101 (Stevens & Haynes, 1907) (analyzing the essential role of citizenship in jurisprudence using the early legal common law).

[26] *See* Stephen Eggleston, *The Myth and Mystery of POGG (Peace order and good government)*, JOURNAL OF CANADIAN STUDIES, Jan. 1, 1996.

[27] Sir Herbert Butterfield, *Raison D'etat—The Relations Between Morality and Government*, Martin Wight Memorial Lecture at the University of Sussex 7 (Apr. 23, 1975) (transcript available at http://www.mwmt.co.uk/documents/butterfield.pdf).

[28] U.S. CONST. art. I, § 9, cl. 2 (The privilege of the writ of habeas corpus shall not be suspended, unless when in cases of rebellion or invasion the public safety may require it).

[29] *See* Boumediene v. Bush, Nos. 06-1195 & 06-1196, 2008 U.S. LEXIS 4887 (U.S. June 12, 2008).

order are restored.[30]

But, for the purpose of our propositions, this approach to the state establishes any state's core interest to control certain fundamental organs or functions that supersede its social contract of competing rights held by its citizens, subjects or members. From the perspective of the Bill of Rights, this *Weberian* state power to override all other rights is a dangerous and blunt authority that should be exercised sparingly and rarely. In fact, U.S. presidents have rarely invoked the Suspension Clause. But it is the proverbial loaded gun that is in the top drawer of any Congress that can be pulled out to allow the state to incarcerate when catastrophic disorder strikes. Moreover, the *Weberian* approach raises the legal potential for the government to claim that borders, due to the power of the state to exercise its authority with impunity, are special and unique locations where the authority of the state is paramount. Historically the borders were concrete, physical and could be demarcated with barriers of fences, flags, planes or ships.

To some critics the emerging world has become a struggle among three types of regimes of legitimacy—the autocratic economies (Russia and China), Islamic traditional states (Iran and Saudi Arabia) and the liberal democracies (U.S. and E.U.).[31] Needless to say, each group has its own internal rivalries but share certain norms and values. Each will continue to struggle to expand power and gather satellites for alliances and to maneuver for comparative advantage. But whither are domestic law and international law in this new world order? In 2006, Craig Allen, an international law professor, hosted a conference of international law experts to "vision" the future of the global legal order in 2020 at the Naval War College.[32] Allen boiled

[30] Note that when President Lincoln suspended the writ of habeas in the Civil War, he worked with Congress and went back to Congress after the fact for post facto approval of the legislature. *See* Lou Fisher, *Invoking inherent powers: a primer*, PRESIDENTIAL STUDIES QUARTERLY, Mar. 1, 2007, *available at* http://www.mywire.com/a/PresidentialStudiesQuarterly//3809872 (last visited Nov. 28, 2008).

[31] Robert Kagan, *The End of the End of History*, NEW REPUBLIC, Apr. 23, 2008, at 40.

[32] For a fuller description of the visions *see* Harvey Rishikof, *National Security Worldview*, THE REPORTER: THE JUDGE ADVOC. GENS. CORPS, Dec. 2006, at 152, 154-55.

down the possibilities of the current global legal order to six possible futures: no growth; slow growth; significant growth; the total disintegration of the order; the fracturing of the order into regional and bilateral arrangements; and, finally, no single future or an order of constant flux.[33] This flux extends to borders and domestic law.[34] In 2008, Russia violated Georgia's borders allegedly to protect the interests of minorities in South Ossetia,[35] while the United States in its war on terrorism crossed borders between Afghanistan and Pakistan under a doctrine of "hot pursuit."[36] How does one assert border control when international law and domestic law allow for "incursions" based on sovereign interpretations? What will citizens or subjects deem legitimate state action in the name of the common defense? Each regime of legitimacy—autocratic economies, Islamic fundamentalist and liberal democracy—views borders as unique areas of sovereign power that trump both domestic and international norms. The state's power is at its zenith, while the individual's zone of privacy and rights is at its nadir.

These propositions have created a social force of extreme state anxiety over border control since the evolving threat to its security (1) runs from economic espionage to weapons of mass destruction, (2) is potentially part of the world communication nodes and (3) is individualized, technologically connected, possibly tied to international criminal networks and centers on the transport of people and goods, the key to globalization. All of these forces and doctrines meet at the border under a state's domestic jurisprudence whereby traditional concepts of privacy stemming form citizenship are most challenged.

---

[33] *Id.*

[34] *Id.*

[35] Mikhail Gorbachev, *Russia Never Wanted a War,* N.Y. TIMES, Aug. 20, 2008, at A23, *available at* http://www.nytimes.com/2008/08/20/opinion/20gorbachev.html?_r=1&oref=slogin&pagewanted=print (last visited Nov. 28, 2008).

[36] Ron Synovitz, *Afghanistan: Legality Of 'Hot Pursuit' Into Pakistan Debated*, June 6, 2008, *available at* http://www.eurasianet.org/departments/insight/articles/pp062308_pr.shtml (last visited Nov. 28, 2008).

II. AMERICAN CONSTITUTIONAL LAW AND PUBLIC POLICY

A. Borders and the Fourth Amendment Strands: Whither Are U.S. Citizenship rights?

The concept of privacy has been an evolving idea in the jurisprudence of the United States. Central to the story has been the interpretation of the Fourth Amendment by the Supreme Court. In many ways our history and the government's attempt to assert order and control over illicit activity and defend against threats to the state by expanding its authority and seeking exceptions to the Fourth Amendment, has defined our contemporary view of privacy. Over the last 100 years, the fight against alcohol in Prohibition, the transportation of women for illicit purposes across state lines, the struggle against anarchism and communism, the anti-war movement, the war against drugs and the combating of terrorism have pitted law enforcement against the civil liberties community.[37] The Supreme Court has crafted rules of the road for law enforcement by setting limits and standards under the Bill of Rights. Critical to the dialogue are the exceptions that have been carved out to allow law enforcement to perform its duty. These exceptions to keep the state's power in check have been extensively litigated and debated. Over time, certain standards have been established to guide law enforcement when violating a citizen's privacy—probable cause, swearing out a warrant, reasonable suspicion and routine administrative searches. Border jurisprudence, however, has been an exception to this concept of privacy.

Professor Thomas K. Clancy has noted that the expansive state border authority has long historical roots; the first customs statute predates the Bill of Rights and allowed for warrantless inspections of vessels.[38] Modern day jurisprudence has similarly

---

[37] *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. R. 349 (1973-74).

[38] *See* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 404, n.22 (2008). *See also* 19 U.S.C. § 482 (2008) (originally enacted as Act of July 18, 1866, ch. 201, § 3, 14 Stat. 178); Immigration and Nationality Act § 287, 8

rejected traditional tests of the totality of the circumstances or heightened levels of suspicion, or minimal indications, or clear indications, or plain suggestions, or articulate suspicion.[39] As Professor Clancy has underscored, for "intrusive" searches and seizures at the border, reasonable suspicion is required.[40] But intrusive has been interpreted to mean unreasonable invasions of the body (body cavity searches, strip searches and x-ray treatment, unless there are facts to give rise to heightened suspicion)[41] or significant damage to property. Border officials, based on training and experience, can conduct a form of targeting that is initially focused on demeanor but then is followed by more extensive investigations, routine "pat downs," searches and inquiries. Federal officers with customs or immigration enforcement authority possess unique power as agents of the state. As has been long noted by courts and traditional law enforcement:

> Congress has given the authority to conduct border searches *only* to this limited group of officials [customs or immigration], and has charged them with the exclusive responsibility for inspecting goods and persons crossing the borders and for interdicting illegal entries. Searches conducted by other law enforcement agents are not considered border searches, . . . and must therefore meet the traditional demands of the fourth amendment.[42]

U.S.C. § 1357 (2008).

[39] *See* United States v. Ramsey, 431 U.S. 606, 619 (1977) (stating that border search exception is older than the Fourth Amendment). *See also* United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985) ("Having presented herself at the border for admission, and having subjected herself to the criminal enforcement powers of the federal government, 19 U.S.C. § 482, respondent was entitled to be free from unreasonable search and seizure."). In *Montoya*, Ms. Hernandez was detained for sixteen hours and had to excrete into a wastebasket since she was suspected of alimentary canal smuggling. *Id.* at 531.

[40] CLANCY, *supra* note 38, at 407.

[41] United States v. Flores, 477 F.2d 608, 609 (1st Cir. 1973) (holding discovery of numerous undeclared emerald stones sufficient for strip search); *see also* YULE KIM, PROTECTING THE U.S. PERIMETER: BORDER SEARCHES UNDER THE FOURTH AMENDMENT (CRS Report, Order Code RL 31826) (updated Jan. 15, 2008).

[42] United States v. Sandoval Vargas, 854 F.2d 1132, 1136 (9th Cir. 1988) (citing United States v. Soto-Soto, 598 F.2d 545, 550 (9th Cir. 1979)).

The customs official's special power to search "vehicles" and "packages" at borders without individualized or reasonable suspicion has been reinforced in the Ninth Circuit by broadly applying 19 U.S.C. § 1581 which allows (1) the search, examination and inspection of vessels and vehicles and (2) examination of manifests, documents, papers, person, trunk, package or cargo on board.[43]

The doctrine has also pushed out the location of borders or extended them. Already in 2004 in one FBI Law Enforcement bulletin the notion of an extend border doctrine was described as follows:

> The extended border doctrine provides that non-routine border searches that occur near the border are deemed constitutionally permissible if reasonable under the Fourth Amendment," something which is determined by a three-part test, "whether 1) there is a reasonable certainty [or a high degree of probability] that a border crossing has occurred; 2) there is a reasonable certainty that no change in the condition of the luggage [i.e., the item or person to be examined] has occurred since the border crossing; and 3) there is a reasonable suspicion that criminal activity has occurred." (50) This three-part test becomes necessary in an extended border search context because it "entails greater intrusion on an entrant's legitimate expectation of privacy than does a search conducted at the border or its functional equivalent[.]" (51) What, however, is reasonable certainty? This is a proof threshold that lies between probable cause and beyond a reasonable doubt. (52) Regarding the second prong of the test, key to concluding whether or not there has been any change in the luggage, conveyance, or any other item, because it crossed the border are factors including "the time and distance from the original entry and the manner and extent of surveillance." (53) The signal characteristic that differentiates the extended border search from one conducted at the border's functional equivalent is that the first "takes place after the first point in time when the entity might have been stopped within the country." (54) Significantly, a proper extended border like a functional

[43] *See* United States v. Taghizadeh, 41 F.3d 1263 (9th Cir. 1994); United States v. Flores-Montano, 424 F.3d 1044 (9th Cir. 2005).

equivalent search may take place without either a warrant or probable cause.[44]

---

[44] *See* M. Wesley Clark, U.S. Land Border Search Authority, Aug. 2004, *available at* http://findarticles.com/p/articles/mi_m2194/is_/ai_n6232025 (last visited Nov. 4, 2008) (internal quotes omitted). Clark's footnotes contained within the above quotation also provide insight regarding this doctrine and are therefore quoted below:

> (50) Yang, 286 F.3d at 945 (emphases added; citations omitted). Of course, one can substitute whatever "container" is at issue for the term luggage. See also United States v. Espinoza-Seanez, 862 F.2d 526, 531 (5th Cir. 1988). The third prong of the extended border test, reasonable suspicion of criminal activity, can arise from a number of factors, to include: "1) characteristics of the area in which the vehicle is encountered; 2) proximity to the border; 3) usual patterns of traffic on the road; 4) previous experience with alien traffic; 5) information about recent illegal crossings in the area; 6) behavior of the driver; 7) appearance of the vehicle; and 8) number, appearance, or behavior of passengers." Espinoza-Seanez, supra at 531; see also Cardenas, 9 F.3d at 1148; ef. Cardona, 769 F.2d at 629 (totality of circumstances test adopted for extended border searches) (citations omitted).
>
> (51) Yang, 286 F.3d at 946 (defendant accosted after he had cleared international arrival terminal, his luggage having been x-rayed with negative results, and had traveled to a separate terminal via airport tram; second look, deemed proper as extended border search, uncovered opium-soaked clothing).
>
> (52) Id. at 947 (citations omitted).
>
> (53) Id. at 948 (citations omitted); see also United States v. Fogelman, 586 F.2d 337 (5th Cir. 1978) (extended border search permitted 254 miles and 20 hours from observed border crossing); United States v. Martinez, 481 F.2d 214 (5th Cir. 1973) (extended border search allowed 150 miles and 142 hours after border was crossed). "[C]ontinuous surveillance is not a requirement of an extended border search[.]" Cardenas, 9 F.3d at 1150, and thus a break in that surveillance is not fatal to the conduct of an extended border search. "The government is not required to negate every hypothetical possibility as to how the contraband may have been obtained subsequent to the border crossing. [T]he mere assertion by the defendant that there was the opportunity to obtain contraband after the border crossing is insufficient to controvert the facts established by the government." Id. at 1152, quoting from Ramos, 645 F.2d at 321 (30-minute break in surveillance does not defeat application of extended border search doctrine). Note that some courts may be confusing functional equivalent and extended border searches. "The 'functional equivalent' subcategory includes searches made at points inland of national borders under circumstances other than continuous surveillance that guarantee preservation of border-crossing conditions at the point of search. The underlying principle that permits them to be treated as border searches is thus the same as that for extended border searches. Courts may in fact be using the terms interchangeably." Bilir, 592 F.2d at 742 n.11.
>
> (54) Cardenas, 9 F.3d at 1148 (original emphasis). There is one characteristic that routine border, border functional equivalent, and extended border searches all have in common: the person, conveyance, or item to be searched "brings the border with it to the point of the search." Id. at 1149 (internal quotation marks and citations omitted).

This physical extension of the border relies heavily on the assumption that surveillance has been able to satisfy the three-pronged test. This notion of extending the physical border has a potential analytical equivalent in the computer world. Moreover as the court established in *United States v. Flores-Montano*, at the border, as part of a routine search, customs officials can dismantle, remove and reassemble a vehicle's fuel tank.[45] As part of the Court's analysis, *Flores-Montano* noted that the search allowed for reassembling and not destruction.[46] The cache of information contained in computers and the possibilities of potential threat enhanced by the justification of border explorations of data presents a powerful potential clash of doctrines.

B. The Clash of the Doctrines?:[47] Extending the Digital Legal Border—All Is Flux

One of the more unfortunate analogies of the post 9/11 era is the alleged hunt "to connect the dots" to thwart any future terrorist attack on continental United States (CONUS).[48] At the outset one must begin with the premise that given the openness of modern society it is virtually impossible to stop all terrorist attacks. The recent histories of attacks in Spain, Great Britain, Israel and France make this premise painfully clear.

Further, any analysis of the cargo shipping industry and its current state of protection, as documented by Stephen Flynn from the Council on Foreign Relations, should underscore his message that resiliency of our infrastructure, not prevention alone, must be the wise policy in the area of combating

[45] 541 U.S. 149, 155 (2004).

[46] *Id.* at 152.

[47] Section drawn from Harvey Rishikof, *The "War on Terror" and Prevention: Improving the Domestic Paradigm for the Digital Age*, NAT'L STRATEGY F. REV., Winter 2007, *available at* http://www.nationalstrategy.com/Programs/NationalStrategyForumReview/PastNSFRIssues/Winter2007NSFRV171/tabid/112/Default.aspx (last visited Nov. 28, 2008).

[48] CNN.com, Testimony of Secretary Condoleezza Rice before the 9/11 Commission, Apr. 8, 2004, *available at* http://www.cnn.com/2004/ALLPOLITICS/04/08/rice.transcript/ (last visited Nov. 28, 2008).

terrorism.[49] With these caveats in mind, the domestic paradigm for investigation of terrorism in the digital age has many facets to which the border exception to the Fourth Amendment provides a heuristic legal and policy analogy.

The current situation of digital investigation is one of a state of flux. Fourth Amendment jurisprudence, data mining, executive authority, war paradigms, due process, border exceptions and judicial review have become a tangled mess for the protection of privacy. In the words of one commentator, modern Internet searches lie at the intersection of telecommunications, spy technology and the statutory regimes that govern surveillance.[50]

It is often said that the U.S. Constitution is a document of enumerated powers, separation of powers, emergency powers and protected rights.[51] The attack on 9/11 has tested competing constitutional theories over where authority lies among these competing powers to respond to the threat of terrorism. Over the last six years this debate has spawned a flurry of legislation, reforms and new institutions—e.g., the PATRIOT Act, Intelligence Reform Acts, a new Department of Homeland Security, a new Director of National Intelligence, a new National Security Branch for the Federal Bureau of Investigation, a secret surveillance program, a new Homeland Security Council and most recent, the Protect America Act. Currently, debate swirls around the new proposed legislation titled the Restore Electronic Surveillance That is Overseen, Reviewed and Effective Act (RESTORE).[52]

Given all these changes, has the United States improved detection, prevention and response? Is more institutional

---

[49] STEPHEN E. FLYNN, EDGE OF DISASTER (2007). Flynn has written extensively on infrastructure security and the importance of resiliency since it is impossible to secure borders given the volume of traffic and the nature of our modern threats.

[50] Barton Gellman, *Conflict Over Spying Led White House to Brink*, WASHINGTON POST, Sept. 14, 2008, at A1, A14.

[51] Robert F. Turner, *The Supreme Court, Separation of Powers, and the Protection of Individual Rights during Periods of War or National Security Emergency*, 28 J. SUP. CT. HIST. 323 (2003).

[52] RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM (Rowman & Littlefield Publishers Inc., 2006).

change needed and how should Fourth Amendment jurisprudence respond? Moreover, has the United States appropriately resolved the tension between civil liberties and investigation? The short answer to these questions is that more change is required and civil liberties may not have been adequately protected.[53]

As outlined in the first part of the paper, over the next few decades there will be certain technological constants. Increasingly, the private sector—telecommunications companies, banks, insurance companies and credit card companies, etc., will be amassing ever larger and more detailed information data banks on U.S. citizens. These ever growing data banks will be subject to even more powerful "search engines" that will able to be "banged" for more connections, relations and ties. It will be the private sector, and not the government, that will be the repository of this critical information.

This information will be carried across borders and sent across borders as digital data by individuals and corporations.[54] The logic of the "data bank banging" argument is that finding terrorists in a sea of information is analogous to the Cold War problem of trying to find Soviet submarines hidden in plain view in the ocean. The solution was to monitor the ocean under normal circumstances and then to register "disturbances." In fighting terrorism the analogy is that a group involved in a conspiracy would emit "patterns of behavior" or "signatures" that would similarly "disturb" the regular flow of commercial behavior and traffic flow. These "patterns" could be identified, and algorithms could be fashioned to pick them out of the sea of "normal" commercial transactions. To be successful though, a "sea" of information is required. This approach was behind the Total Information Awareness Program (TIA) established at the Department of Defense's Defense Research Projects Agency (DARPA) that caused a political firestorm when it was

[53] *See, e.g.*, Symposium, *Left Out in the Cold? The Chilling of Speech, Association, and the Press in Post-9/11 America*, 57 AM. U. L. REV. 1197 (2008).

[54] *See supra* text accompanying note 23.

revealed.[55] The goal of the TIA program was "to create a counter-terrorism information system that: (i) increase[d] the information coverage . . . (ii) provide[d] focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; [and] (iii) [could] automatically cue analysts based on partial pattern matches and analytical reasoning, and information sharing . . . ." [56] As outlined by the Congressional Service Report:

> DARPA's five year research project to develop and integrate information technologies into a prototype system for use by the intelligence, counterintelligence and law enforcement communities intends to exploit R&D efforts that had been underway for several years in DARPA and elsewhere, as well as private sector data mining technology. DARPA envision[ed] a database "of an unprecedented scale, [that] would most likely be distributed, must be capable of being continuously updated, and must support both autonomous and semi-automated analysis." . . . Extensive existing databases from both private and public sector information holdings [would have been] used to obtain transactional and biometric data. Transactional data for the TIA database could include financial (*e.g.*, banks, credit cards, and money transmitters, casinos and brokerage firms), educational, travel (*e.g.*, airlines, rail, rental car), medical, veterinary, country entry, place/event entry, transportation, housing, critical resources, government, and communications (*e.g.*, cell, landline, Internet) data. Biometric data for the database could include face, finger prints, gait, and iris data. The TIA system could seek access to databases to discover connections between "passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases—and events—such as arrest or suspicious

[55] *See* ACLU, Stunning New Report On Domestic NSA Dragnet Spying Confirms ACLU Surveillance Warnings, *available at* http://www.aclu.org/privacy/gen/34441prs20080312.html (last visited Oct. 10, 2008) (ACLU's response to the TIA).

[56] *See* Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, CONG. RES. SERV., Mar. 21, 2003, at 2, *available at* http://www.fas.org/irp/crs/RL31730.pdf (last visited Oct. 22, 2008) (citations omitted).

activities and so forth."[57]

In the end Congress requested that the program be stopped—but the logic that underlies the approach lives, and border crossing has become the next focal point of the debate for information gathering.[58]

C. Electronic Surveillance, Searches and Foreigners

If prevention of terrorism, however, is the goal of the state, then timely information to thwart actions is the key to success. The recent debate over the RESTORE legislation is a perfect example of the interrelated issues of data mining, prevention and digital borders.[59] The new National Security Letters, for example, granted to the FBI under the PATRIOT legislation, allow local agents to request data, without any court order, from the private sector.[60] In short the border for information acquisition was moved, without judicial supervision, closer to executive discretion.

Domestically the debate asked various questions related to the proper legal procedure for acquiring access to these data banks: Should the executive branch [on its own authority to protect the republic] be able to request the records in order to search them without judicial oversight? Should the private

[57] *Id.* The federal laws triggered by the approach included the following: The Privacy Act of 1974, The Family Educational Rights and Privacy Act of 1974, The Cable Communications Policy Act of 1984, The Video Privacy Protection Act of 1988, Telecommunications Act of 1996, The Health Insurance Portability and Accountability Act of 1996, Driver's Privacy Protection Act of 1994, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, The Foreign Intelligence Surveillance Act of 1978, The Electronic Communications Privacy Act of 1986, The USA PATRIOT Act of 2001, The Homeland Security Act of 2002, The Fair Credit Reporting Act of 1970, The Right to Financial Privacy Act of 1978, The Gramm-Leach-Bliley Act of 1999, and The Children's Online Privacy Protection Act of 1998. *Id.* at 6-16.

[58] *See* JAMES BAMFORD, THE SHADOW FACTORY, THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA, (Doubleday, 2008) (discussing the latest revelations concerning the National Security Agency).

[59] *See* ThinkProgress, *available at* http://thinkprogress.org/restore-act-summary/ (last visited Oct. 21, 2008) (providing summary of the RESTORE Act of 2007).

[60] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 18 U.S.C. § 2709 (2008), *invalidated by* Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

companies that cooperate be able to be sued, or should they be granted immunity from lawsuits? What level of suspicion should be required before access is granted to these data bases—individual, as traditionally required by the Fourth Amendment, or a more general class identification (e.g., all the records from all the hotels in Las Vegas where a threat to the city is suspected)? The RESTORE debate wrestled with these questions.[61] In effect, the debate from the government's perspective was an attempt to philosophically extend digital "border" protection to the interior of the state.

Politically, this constitutional question of the governmental right to search, and under what standard of review, will continue to bedevil any administration that plans to combat terrorism. Where will the constitutional authority lie and what should be the role of the courts in the process? In the physical border context the discretion falls on the border agents. Proponents of a strong executive argue that when the state is at war, such as the war on terrorism, the commander-in-chief has constitutional authorization to initiate terrorist surveillance programs based on his inherent authority.[62] This inherent authority trumps all restraints, even if Congress has legislated in the area and mandated judicial review of the process.[63] This approach grants and extends custom and immigration warrantless search authority inwards and erodes the U.S./non-U.S. distinction that has been such a vital component of our constitutional framework.

Opponents to this position reason that this is a congressional prerogative and once Congress has established the rules to govern the situation, the president is bound to follow them, or risk censure, or even impeachment. For this view of constitutional power, unchecked executive power in the defense

---

[61] *See, e.g.*, The Huffington Post: Blog of U.S. Rep. Rush Holt, *available at* http://www.huffingtonpost.com/rep-rush-holt/whats-really-in-the-rest_b_74309.html (Nov. 27, 2007, 12:33 EST).

[62] *See, e.g.*, Dawn E. Johnson, *What's a President to Do? Interpreting the Constitution in the Wake of Bush Administration Abuses*, 88 B.U. L. REV. 395, 395-96 (2008) (criticizing the position).

[63] *Id.*

of liberty results in problems such as the Palmer raids of the 1920s, the miscarriage of justice under the McCarthy era in the 1950s, and the violations of civil liberties uncovered by the Church Committee in the 1970s.[64] In fact, to many it was these very executive violations that spurred Congress to pass the Foreign Intelligence Surveillance Act (FISA) in 1978.[65]

FISA, however, was drafted in an era before the technological revolution of the Internet and when a separation of domestic and foreign arenas was taken for granted. At the heart of the FISA legislation was the distinction between a U.S. citizen and a non-U.S. citizen. In many ways technology, the U.S./non-U.S. citizen distinction and the separation of domestic and foreign spheres has been undermined by the evolution of communication and the nature of the evolving threat. FISA envisioned a world of states v. states, not a world of stateless actors working in cooperation to attack CONUS, with some of the enemies potentially being U.S. citizens. This type of threat that has been successful in Spain and Great Britain is a challenge to the old order and legal structures. Border jurisprudence, as part of our founding, never distinguished between U.S. and non-U.S. citizens in the Fourth Amendment sense. At the border U.S. citizens have a reduced sense of Fourth Amendment protection. The debate of what protection a computer has at the border is one that raises legal issues over how to understand what digital datum is. Again, Professor Thomas K. Clancy has elegantly argued that electronic data on a computer does not require a "special approach" and should be governed by traditional Fourth Amendment rules regulating containers and document searches.[66]

FISA's solution was, when dealing with non-U.S. citizens, to involve the federal judiciary to curtail executive power in the area of foreign persons or agents of foreign entities. In a system parallel to the criminal process, where search warrants

---

[64] *See* DAVID COLE, ENEMY ALIENS, (W.W. Norton & Co. photo reprint 2005) (2003).

[65] *See* Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C. & 18 U.S.C. §§ 2518-2519).

[66] Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193 (2005).

requiring probable cause of a crime obtained from a federal judge are needed, FISA requires probable cause of a "foreign agent" before surveillance can be established.[67] The lack of U.S. status became the critical threshold before monitoring could take place. What has changed for proponents of executive power to argue that the judiciary should not be involved in this procedure? In short, the government claimed that it stood in the shoes of a customs or immigration official and that at the technological border—no Fourth Amendment was a bar to state action.

The position to exclude the judiciary in the process of monitoring surveillance rests on arguments of constitutional authority and necessity. First, proponents argue that the United States is at war and this authority to protect is a presidential right that cannot be curtailed.[68] If the President approves the authorization it is constitutionally appropriate under his emergency war powers. Second, proponents believe that judges lack the institutional competence to second-guess the executive on its judgments when the United States is at war and when protection of the homeland is paramount.[69] Third, in this era of technological information, speed, surveillance and data mining are the keys to prevention, and proponents argue this too is beyond the judiciary's competency.[70] The world of exploiting information has changed and the judicial review is not useful, since a deliberative procedure is the antithesis of prevention based on speed of action and establishing connections.

The response to these arguments is a flat rejection of the premises for each of the positions. Philosophically, supporters of the judiciary are wedded to the Madisonian principle of checks and balances. No branch, when civil liberties are involved,

---

[67] *See* 50 U.S.C. § 1802(a)(1)(A) (1978).

[68] See, John Yoo, *Exercising Wartime Powers The Need for a Strong Executive*, HARV. INT'L REV., *available at* http://www.harvardir.org/articles/1369/1/ (last visited Nov. 28, 2008).

[69] *See* The Federalist Society Online Debate Series, FISA, Dec. 11, 2007, *available at* http://www.fed-soc.org/debates/dbtid.13/default.asp (last visited Nov. 21, 2008).

[70] *Id.*

should be granted sole authority. To this school, terrorism is more of a criminal matter rather than one of war. Europe has taken this approach by passing expanded criminal statutes to combat terrorism.[71] For the Madisonian proponents, the judiciary should be second-guessing the executive. This school points to the violations of the FBI in using National Security Letters, as documented by the Inspector General of the Department of Justice, to underscore why the judiciary must be part of the process.[72] Finally, on the issue of speed, the proponents for the role of judges reason there are ways to expedite the processes. After the fact, once decorum has been reestablished, a backward-looking review under judicial scrutiny can be undertaken to right any wrongs.

After months of negotiations and wrangling on these issues, Congress secured passage of the Foreign Intelligence Surveillance Act of 2008 (FISA/2008).[73] Critics of the Act have focused on several issues: the retroactive civil and criminal immunity granted to telecommunications corporations for compliance with executive requests that arrived without court orders; the more restricted certification process for the reviewing FISA court; the broader "dragnet" broadband authorization for information; and the expanded reporting time granted the government.[74] Defenders of the legislation emphasize the clear statement that the new FISA/2008 is the "exclusive means" for intercepting electronic communications; increased congressional oversight; the enhanced protections for U.S. citizens living overseas; and the new enhanced role of the inspector general to

[71] *See* Prepared Remarks of Attorney General Alberto R. Gonzales at the Vienna E.U. Interior Ministers Conference, May 5, 2006, *available at* http://www.usdoj.gov/archive/ag/speeches/2006/ag_speech_060505.html (last visited Nov. 21, 2008).

[72] *See A Review of the FBI's Use of National Security Letters*, DEP'T OF JUSTICE SPECIAL REP., Mar. 2008, *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf (last visited Nov. 28, 2008).

[73] *See* The FISA Amendments Act of 2008, 50 U.S.C. § 1802 (1978), *amended by* H.R. 6304 (2008).

[74] *See* ACLU website *at* http://www.aclu.org/safefree/general/17321res20030408.html (last visited Nov. 28, 2008).

review the government's actions.[75]

Regardless of where one breaks on the issues, there appears to be a consensus that FISA needs to be modernized to account for the new technologies and developments in the communications arena. The "old" FISA of 1978 was written for a world of phones, routers and telegraphs with limited traffic capacities and specific locations whereby one could clearly delineate foreign and domestic. The brave new world of web-based communications has revolutionized technical mechanisms, delivery modes, locations, storage banks and volume. The lapsing stop-gap Protect America Act, the limited fix to FISA, recognized that something new was needed.[76] A new approach was required for an increasingly borderless world of communications, mobile citizenry and data storage facilities.

Knowable individualized surveillance versus general broadband collection is an essential part of the debate—who will authorize the broadband collection, by what standards, and who will review the authorization and monitor the collection? This is often referred to as the "minimization" issue—in short, how and who will keep the executive accountable. As David Kris, a former Associate Deputy Attorney General who has written extensively on national security issues and surveillance, has pointed out FISA/2008 has three essential substantive requirements: first, a target that is a foreign power or an agent of a foreign power; second, a facility being used by that target; and third, minimization.[77] To satisfy these requirements without sacrificing speed and agility, it is necessary to identify the broadest possible target and facility, which will yield the broadest possible authorization order and require the fewest

[75] CRS Report, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, June 12, 2008 (RL 34533), *available at* http://www.fas.org/sgp/crs/intel/RL34533.pdf (last visited Nov. 28, 2008).

[76] *See Fact Sheet: The Protect America Act of 2007*, OFF. PRESS SEC'Y, Aug. 6, 2007, *available at* http://www.whitehouse.gov/news/releases/2007/08/print/20070806-5.html (last visited Nov. 28, 2008).

[77] *See* Posting of David Kris to Balkinization, *available at* http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-i.html (June 21, 2008, 8:50 EST).

possible court orders for the most surveillance.[78]

These facilities or international gateway switches have enormous amounts of data and traffic. But the status of the origin of the communication, the nationality of the communicator and the storage location of the data challenged the old FISA categories of target and facility. What are domestic-to-domestic versus international-to-domestic versus international-to-international communications? Imagine an American traveler who lends his iPhone to a French friend to make a call from Germany to his friend in Yemen. This call would now require a FISA warrant if the American was a target.

The Bush administration, confronted with the problem of identifying the nationality of the communicator, the location of the communicator, the place of the "facility" and volume of the data, chose to ignore the old FISA.[79] The administration asserted executive presidential prerogative to use the foreign power/foreign origin of the communication to assert that it did not need a FISA warrant to secure the data from the owners of the international gateway switches and stored data banks.[80] The potential threat, the administration reasoned, warranted swift action.[81]

The next step was to use "filters" or "data searches" to find the communication network needle in the haystack. Under the minimization doctrine and the new act, the government is to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[82] But if the data is "foreign intelligence information" or is "evidence of a crime which has been, is being, or is about to be committed," it can be retained and acted upon.[83] This has raised concerns in the civil

---

[78] *Id.*

[79] *See* Julian Borger & Suzanne Goldenberg, *Defiant Bush Defends Wiretapping Powers*, THE GUARDIAN, Dec. 20, 2005, *available at* http://www.guardian.co.uk/world/2005/dec/20/usa.topstories3 (last visited Nov. 28, 2008).

[80] *Id.*

[81] *Id.*

[82] *See* 50 U.S.C. § 1801(h) (1978).

[83] *See* 50 U.S.C. § 1802 (1978), *amended by* H.R. 6304 (2008).

liberty community about how much information these sweeps will gather.

The new FISA is an attempt to bring back accountability and review of governmental action in this complex technical area of electronic surveillance in the digital age. But as this brief review has highlighted, it is the technology that has made obsolete so many of the categories of the old FISA. The concept of U.S. citizen is harder to determine in this interconnected world of mobile communications and storage capacities. The modern world is creating enormous data banks of information controlled by the private sector. The government is only a warrant or a subpoena away from this vast ocean of information on its citizens and visitors. All governments are wrestling with the problem of how, under the rule of law, information should be obtained, searched, protected and not be the subject of governmental abuse. The new FISA statute is the most recent attempt to resolve these problems, but many questions remain to be answered as the intelligence community begins to "operationalize" the new rules.

The data is there in the private sector. Technology allows for more extensive and detailed searches. The goal is to prevent the threats; the government is held accountable for failures. As one can see, the FISA debate is more than a debate about technology, modern surveillance and executive accountability. At the heart is the erosion of citizenship as a shield to government intrusion and what privacy means in the new age. Congress has entered the fray again with more review; the IGs are part of the process; and the FISA court's authority has been reinstated. The hope is that more judicial review will provide enough accountability; but, a new president will have to see if the framework is adequate.

D. Are We At War?: If So, What Kind of War?

Since the passing of the Authorization for the Use of Military Force (AUMF) by joint resolution of the Congress in 2001, the invasion of Afghanistan, Iraq and by incursions into Pakistan, the Administration has contended the republic is at

war.[84] Most significantly for the theory of the clash of doctrines, the AUMF for the first time in U.S. history, authorized "all necessary and appropriate force" against "those nations, organizations, or persons" the President determined were responsible for the acts and similar force to prevent the occurrence of future acts. The power of the state could be focused on specific individuals; this was a fundamental change in how, and from whom, threats were conceived. In essence, the AUMF has ushered in a new paradigm of conflict and state power.

For it is an old saw that military or security "necessity" justifications, when civil liberties are encroached, should be viewed with a "healthy skepticism."[85] As has been pointed out by Judge James E. Baker in exploring the meaning of national security, there is "no single definition of national security" recognized in law or policy and "[s]ecurity is concrete [while a] [r]ule of law is an abstraction, a term that is easy to employ in rhetoric, but hard to measure in result."[86] As underscored by

[84] Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001). AUMF reads in relevant part as follows:

> To authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States. Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it . . .
>
> SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.
>
> (a) IN GENERAL- That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

[85] *See* Brown v. Glines, 444 U.S. 348, 369 (1980) (Brennan, J., dissenting).

[86] JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 18, 22 (Cambridge University Press 2007).

Baker, Justice Jackson once famously opined, "a judge . . . may be surprised at the poverty of really useful and unambiguous authority applicable to concrete problems of executive power as they actually present themselves."[87] Faced with the dilemma of "concrete security" versus "abstraction in law," policy makers are prone to choose the concrete at the expense of abstraction. But again, Baker's words are prescient:

> . . . a national security policy that does not include the rule of law as a core element will diminish not only our liberty but also our security. That is because good process, founded in law, including good legal process, as well as good faith adherence to the law, produces better security results.[88]

From the founding of the republic, Alexander Hamilton in Federalist Paper No. 8 judiciously warned that it is the nature of war to increase the executive at the expense of the legislative authority.[89] How to avoid this executive expansion of power under the cloak of security necessities? One answer is a full vetting process by the executive whereby all affected parties have an opportunity to voice views. Baker previewed the recent legislation on electronic surveillance in his review of constitutional law as applied. In a creative chapter, Baker (in lawyer-like fashion) lays out the legal arguments for and against presidential authority to authorize warrantless surveillance under the Foreign Intelligence Surveillance Act (FISA). He based his arguments on an analysis of the legal categories of a constitutional framework/court precedents/wartime powers and responsibilities/historic practices/statutory analysis under FISA, the Authorization to Use Military Force (AUMF), and facts.[90] This analysis is followed by an equally powerful "legal policy advice" section presenting the prudential factors in determining the President's position to exercise "inherent executive power" based on secrecy, efficiency, presidential authority and

---

[87] *Id.* at 47.

[88] *Id.* at 22.

[89] THE FEDERALIST NO. 8 (Alexander Hamilton).

[90] BAKER, *supra* note 86, at 71.

legislative tactics.[91] Again he explores in the alternative, the following of a parallel track with the legislature or judiciary based on rule of law and public diplomacy/sustained public support/maximization of presidential authority/encouraging risk-taking with legislative backing/ and most prophetically private sector protection and support.[92] The point is a deliberative process with checks and balances. If the new electronic frontier borders require surveillance, then Congress, as it recently has done, must involve the judiciary as a check on potential executive abuse. In the alternative, the executive, when perceiving catastrophic threats will opt for a physical border approach and push for more Fourth Amendment exceptions.

But the issue remains when at the border with a computer: What are the government's interests, and what is a reasonable expectation of privacy? Moreover, if the data is encrypted, by what manner should the border guards be able to request the password? Under the container theory, encryption is analogous to a lock, and failure to provide the key allows border detention and refusal to be admitted. The levels of issues range from national security justifications, to stopping pornographers, to new creative ways to launder money using Second Life programs, to economic espionage.[93] Computers at the border potentially contain material for all of these threats and crimes. The issue of computers at the border raises questions of sovereignty, technology, citizenship, national security, and privacy rights. In short, it presents a clash of legal and political doctrines over sovereignty and the limits of state power over the individual.

E. Smart Borders: Immigration, Privacy and Rights

It is instructive in understanding this clash of doctrines to

---

[91] *Id.* at 94.

[92] *Id.* at 95.

[93] *See* John S. Grant IV, *The New Frontier in the Fight Against Online Economic Scams and Internet Threats to Children: Virtual Worlds and Second Life*, CYBERCRIME NEWSLETTER, July-Aug. 2008, at 3.

review the latest advice from the National Counterintelligence Executive Office (NCIX) on what you should know when traveling overseas with mobile phones, laptops, PDAs and other electronic devices. In other words, how our friends and foes are treating borders and searches:

> • In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel businesses centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
>
> • All information you send electronically—by fax machine, personal digital assistant (PDA), computer, or telephone—can be intercepted. Wireless devices are especially vulnerable.
>
> • Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this remove the battery.
>
> • Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.
>
> • Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other "gifts."
>
> • Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.
>
> • Corporate and government officials are most at risk, but don't assume you are too insignificant to be targeted.
>
> • Foreign security services and criminals are adept at "phishing"—that is, pretending to be someone you trust in

order to obtain personal or sensitive information.

• If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, you should assume the device's hard drive has been copied.[94]

This advice is both disturbing and an insight into how the intelligence community understands borders and technology in the twenty-first century. This sense of vulnerability has also encouraged a refocus on travel documents since "[f]or terrorists, travel documents are like weapons."[95] The Department of Homeland Security, in an attempt to secure borders and identification, supported the REAL ID Act of 2005[96] and the Western Hemisphere Travel Initiative (WHTI).[97] As a result, in 2007 more than 30,000 individuals were detained at ports of entry trying to cross the border with false documents.[98] Under the REAL ID Act, each card must include, at a minimum, the person's full legal name, signature, date of birth, gender and

[94] Tips from the National Counterintelligence Executive, *Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices*, NCIX, Aug. 5, 2008, *available at* http://www.ncix.gov/whatsnew/index.html (last visited Nov. 28, 2008).

[95] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 108TH CONG., 9/11 COMMISSION REPORT 384 (Comm. Print 2004).

[96] Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami

Relief, Pub. L. No. 109-13, 119 Stat. 231 (2005); *see also* The Legislation Behind a National ID, CNet News, *available at*

http://news.cnet.com/The-legislation-behind-a-national-ID/2100-1028_3-6228910.html?tag=txt (last visited

Oct. 27, 2008). For example, in 1995 Timothy McVeigh, the Oklahoma bomber of the Murrah Federal Building, created a fake South Dakota driver's license using a manual typewriter and a kitchen iron. He then used this fake license to rent the Ryder truck he filled with explosive material. Baker, *infra* note 97.

[97] Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec., Statement for the Record Before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, United States Senate, (April 29, 2008), *available at* http://hsgac.senate.gov/public/_files/BakerTestimony042908.pdf (last visited Nov. 28, 2008).

[98] *Id.* at 4.

driver's license or identification card number.[99] It also includes a photograph of the person's face and the address of principal residence, as well as physical security features designed to prevent tampering, counterfeiting or duplication of the document for fraudulent purposes.[100] Although the DHS denies that the REAL ID Act creates a national identification card, critics contend that the law places no limits on potential required uses for Real IDs. The fear is that in the future:

> Real IDs could be required to vote, collect a Social Security check, access Medicaid, open a bank account, go to an Orioles game, or buy a gun. The private sector could begin mandating a Real ID to perform countless commercial and financial activities, such as renting a DVD or buying car insurance. Real ID cards would become a necessity, making them de facto national IDs.[101]

Would the creation of a national ID card be the end of privacy? Many democratic European countries have had national IDs for decades and are introducing new "biometric IDs," but how would the national IDs be monitored by the state?[102]

Under the WHTI Air Rule all arriving air travelers, regardless of age, are required to present a passport or other acceptable secure document for entry into the United States. Since the rule has been adopted, compliance is over ninety-nine percent for citizens of the United States, Canada and Bermuda. The conclusion is that Americans and foreign nationals alike are willing to obtain the necessary documents to enter or re-enter the United States once the requirements are known and enforced. In short, more documentation and cross-cutting databases are in the future for border crossings; at the same

---

[99] *See supra* note 96.

[100] *Id.*

[101] American Civil Liberties Union, ACLU of Maryland Blasts New Real ID Regulations, *available at* http://www.aclu.org/privacy/gen/33952prs20080115.html http://www.aclu.org/privacy/gen/33952prs20080115.html (last visited Oct. 27, 2008). Needless to say a number of states have opted out of enforcing the ID.

[102] BBC News, Foreign National ID Card Unveiled, *available at* http://news.bbc.co.uk/2/hi/uk_news/politics/7634111.stm (last visited on Oct. 27, 2008).

time, any expectation of privacy or protection due to citizenship is severely diminished, if not extinguished. In the words of Stewart Baker, Assistant Secretary for Policy of the DHS, "[t]he development, production, and distribution of quality, physically secure documents, is an expensive process, as it requires replacing old document production systems and infrastructure; however, the investment will pay healthy dividends towards the security of this country."[103]

These programs flow from the 9/11 Report that recommended: 1) creating a strategy to combine terrorist intelligence, operations, and law enforcement; 2) integrating the U.S. border security system into a larger network of screening points; 3) implementing a biometric entry-exit screening system; and 4) enhancing international cooperation, particularly with Canada and Mexico.[104] The reason for the need of a technological web of connectivity recommended by the 9/11 Commission turns on the volume traffic and the size of the border. The United States has nearly 100,000 miles of shoreline and almost 6,000 miles of borders with its neighbors.[105] People and goods arrive daily at more than 3,700 terminals in 301 ports of entry.[106] To find "one man" amid the approximately 500 million people, 125 million vehicles and 21.4 million import shipments that came into the country last year, with 6 million cargo containers, 2.2 million rail cars and 11.2 million trucks "is about as likely as winning a lottery."[107]

The government's continuing commitment to win the lottery with border control and stem immigration is demonstrated by the 2007 Secure Border Initiative or SBInet which will deploy "a mix of personnel, technology, infrastructure

---

[103] Baker, *supra* note 97, at 5-6.

[104] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 385-90 (official gov't ed. 2004); s*ee also* YULE KIM, PROTECTING THE U.S. PERIMETER: "BORDER SEARCHES" UNDER THE FOURTH AMENDMENT 16 (CRS Report, Order Code RL 31826) (updated Jan. 15, 2008).

[105] Stephen E. Flynn, *Beyond Border Control*, 79 FOREIGN AFF. 57 (Nov./Dec. 2000).

[106] *Id.*

[107] *Id.*; *see also* Roberto Iraola, *Terrorism, the Border, and the Fourth Amendment*, 2003 FED. CTS. L. REV. 1 (2003).

and response assets"[108] with a multi-billion dollar set of 300 miles of fencing and the potential for unmanned aerial vehicles patrolling the borders with high definition cameras currently deployed on the battlefields of Iraq and Afghanistan.[109] The goal is to create "smart borders" with electronic registration systems, visa programs and waiver systems for safe travelers.[110] It is estimated that there are between 11 and 12 million illegal immigrants in the United States. In early 2002, the Immigration and Naturalization Service director estimated that to control the border the department would need 27,000 investigators and special agents (at the time there were 2,000); 31,000 Border Patrol agents (in 2008 there are 18,000); 21,500 immigration inspectors (compared to 5,000); 15,600 deportation officers (compared to 650); 1,440 attorneys (compared to 777) and 110,000 detention beds (compared to 33,000 in 2008).[111] The cost and numbers are staggering. This confusion or clash of immigration policy with preventing terrorism underscores why the doctrines need to be thought through carefully and analytically, to truly create a "smart border."[112] Smart visa and passport tracking is essential since as pointed out by one of the more outstanding monographs produced by the 9/11 Commission, documentation was key to the attackers:

---

[108] *See* BLAS NUNEZ-NETO & YULE KIM, BORDER SECURITY: BARRIERS ALONG THE U.S. INTERNATIONAL BORDER 27-28 (CRS Report, Order Code RL 33659) (updated May 13, 2008). This report details the scores of acts that were waived by Congress to speed the construction of the San Diego fences and walls from the Federal Water Pollution Control Act to the Administrative Procedure Act. *Id.* at 47-48.

[109] JASON BLAZAKIS, BORDER SECURITY AND UNMANNED AERIAL VEHICLES 2 (CRS Report, Order Code RS 21698) (updated 2008).

[110] *See* Kenn Morris, *Moving Toward Smart Borders*, June 2003, *available at* http://www.sandiegodialogue.org/pdfs/Asa_Paper_June_03.pdf (last visited Nov. 28, 2008). Visa and tracking programs include: National Security Entry-Exit Registration System (NEERS), Student and Exchange Visitor System (SEVIS), etc.

[111] EDWARD ALDEN, THE CLOSING OF THE AMERICAN BORDER 297 (2008).

[112] *See* Susan Ginsburg, *Weaknesses In The Visa Waiver Program: Are The Needed Safeguards In Place To Protect America?*, Testimony Before the Senate Judiciary Committee, Subcommittee on Terrorism, Technology & Homeland Security (Feb. 28, 2008), *available at* http://www.homeland.ca.gov/pdf/testimony/senate/sju/02-28-08/Testimony_SusanGinsburg_TheMigrationPolicyInstitute.pdf (last visited Nov. 28, 2008).

> The success of the September 11 plot depended on the ability of the hijackers to obtain visas and pass an immigration and customs inspection in order to enter the United States. It also depended on their ability to remain here undetected while they worked out the operational details of the attack. If they had failed on either count—entering and becoming embedded—the plot could not have been executed.
>
> Here we present the facts and circumstances of the hijackers' travel operation, including their 25 contacts with consular officers and their 43 contacts with immigration and customs authorities. We also discuss the 12 contacts with border authorities by other September 11 conspirators who applied for a visa. The narrative is chronological, retracing the hijackers' steps from their initial applications for U.S. visas, through their entry into the United States, to their applications for immigration benefits, and up through their acquisition of state identifications that helped them board the planes. Along the way, we note relevant actions by U.S. government authorities to combat terrorism. There were a few lucky breaks for U.S. border authorities in this story. Mostly, though, it is a story of how 19 hijackers easily penetrated U.S. border security.[113]

Legal doctrine, however, in the border context continues to expand the use of new technology for state use. In 2007, the Director of National Intelligence designated DHS as the agent for the National Applications Office (NAO) to run satellite imagery over the United States.[114] A set of pre-9/11 Supreme Court cases explored imagery and the Fourth Amendment.[115] In *California v. Ciraolo*, the Court in a 5-4 decision held that warrantless aerial observation from 1,000 feet of a fenced-in-backyard containing marijuana did not constitute a search.[116]

---

[113] *See* Thomas R. Eldridge, Susan Ginsburg, Walter T. Hempel II, Janice L. Kephart, & Kelly Moore, *9/11 and Terrorist Travel*, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *available at* http://govinfo.library.unt.edu/911/staff_statements/911_TerrTrav_Monograph.pdf (last visited Nov. 28, 2008).

[114] RICHARD A. BEST JR & JENNIFER K. ELSA, SATELLITE SURVEILLANCE: DOMESTIC ISSUES 7 (CRS Report, Order Code RL 34421) (updated on Mar. 21, 2008).

[115] *Id.* at 14-16.

[116] California v. Ciraolo, 476 U.S. 207 (1986).

On the same day, the Court also held in *Dow Chemical Co. v. United States* that aerial photography of an industrial compound from a greater altitude by government regulators, in navigable airspace using a specialized camera, was similarly not a search.[117] Some Justices on the Court, however, noted that if the compound had been a private home or the camera had been a unique sensory device able to penetrate the walls, a warrant might have been required.[118] Finally in *Florida v. Riley*, in a plurality opinion, the Court concluded that a police helicopter hovering at 400 feet in a surveillance flight observing through a greenhouse roof marijuana growing was not a Fourth Amendment violation.[119]

Naturally, in the context of the United States, using Department of Defense (DOD) assets such as satellite imagery raises potential violations of the Posse Comitatus Act.[120] In 1991, the Office of Legal Counsel in the Department of Justice opined, however, that the use of military personnel to conduct aerial infrared monitoring of private property for law enforcement purposes (assisting DEA in monitoring illicit narcotics production) was not a violation of the Posse Comitatus because the surveillance was not a search, seizure or arrest since there was no "physical contact" resulting in a direct confrontation between military and civilians.[121] Given the "border exception" and the "national security" considerations, the real questions for satellite imagery are not the constitutional ones — they appear to have been answered — but rather the policy ones posed by the report: How much "valued added" is satellite imagery? Is congressional oversight adequate? And, how does the government ensure that the NAO operates within the governing statutes for the intelligence agencies?[122] As in the

[117] Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[118] *Id.* at 237 n.4, 238. *See also id.* at 243 n.4 (Powell, J., dissenting).

[119] Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion).

[120] Posse Comitatus Act, 18 U.S.C. § 1385 (2008).

[121] Military Use of Infrared Radars Technology to Assist Civilian Law Enforcement Agencies, 15 U.S. Op. Off. Legal Counsel 36 (1991), *quoted in* BEST & ELSA, *supra* note 114, at 22-23.

[122] BEST & ELSA, *supra* note 114, at 25-26.

FISA example under the border exception cases, how does one monitor or maintain the US/non-US citizenship distinction on the border, "extended border" or "functional border" with satellite technology? The clash of doctrines at the border begin to converge as the power of technology allows for greater transparency by the state based on the threat of the individual at the price of immigration movements, privacy, autonomy and citizenship protections.

This quest and search of "actionable" intelligence, a smart border and the border exception has come together on laptop searches. In *United States v. Arnold*, the lower court in suppressing the evidence for trial found that "opening and viewing confidential computer files implicates dignity and privacy interests" and could not fall under the routine inspection border exception but required "reasonable suspicion."[123] Under the facts of the case, U.S. Customs and Border Patrol first questioned Arnold returning from the Philippines, booted up his computer, clicked on folders titled "Kodak Pictures" and "Kodak Memories" and found pictures of nude women.[124] Immigration and Customs Enforcement agents were then called in; they detained Arnold for several hours, continued to examine the computer and found what they believed to be child pornography.[125] The Court of Appeals in reversing the lower court's order to suppress the evidence re-emphasized the distinction the Supreme Court has established in its "border"

[123] United States v. Arnold, 454 F. Supp. 2d 999, 1003 (C.D. Cal 2006).

[124] *Id.* at 1001.

[125] *Id.*

> A grand jury charged Arnold with: (1) "knowingly transport[ing] child pornography, as defined in [18 U.S.C. § 2256(8)(A)], in interstate and foreign commerce, by any means, including by computer, knowing that the images were child pornography"; (2) "knowingly possess[ing] a computer hard drive and compact discs which both contained more than one image of child pornography, as defined in [18 U.S.C. § 2256(8)(A)], that had been shipped and transported in inter-state and foreign commerce by any means, including by computer, knowing that the images were child pornography"; and (3) "knowingly and intentionally travel[ing] in foreign commerce and attempt[ing] to engage in illicit sexual conduct, as defined in [18 U.S.C. § 2423(f)], in a foreign place, namely, the Philippines, with a person under 18 years of age, in violation of [18 U.S.C. § 2423(c)]."

United States v. Arnold, 523 F.3d 941, 943 (9th Cir. 2008).

jurisprudence of "particularized suspicion" between searches of the "person" versus those involving "property."[126] The appellate court reasoned that computers are more like vehicles or property than objects with special "privacy interests" that would trigger an "intrusiveness analysis" of the person as in a body cavity search.[127] The appellate court went on to note that the Supreme Court's other two narrow exceptions to a search, when "exceptional damage to the property" had taken place or when the search was "particularly offensive," had not been triggered by the mere booting up the computer.[128] The court further rejected any claim that the computer could be thought of as "capable of functioning as a home" for a Fourth Amendment analogy.[129] Finally, the court approvingly cited a Fourth Circuit case, *United States v. Ickes*, in which the defendant's van was searched and a video camera containing a tennis match that "focused excessively on a young ball boy" prompted a more thorough examination of the van where more prepubescent pornography was uncovered.[130] The Fourth Circuit rejected any First Amendment defense in the *Ickes* case, particularly given the threat of terrorism.[131] The *Arnold* court was persuaded by the analysis and followed its reasoning:

> The Fourth Circuit held that the warrantless search of defendant's van was permissible under the border search doctrine. The court refused to carve out a First Amendment exception to that doctrine because such a rule would: (1) protect terrorist communications "which are inherently 'expressive'"; (2) create an unworkable standard for government agents who "would have to decide—on their feet—which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First

[126] *Arnold*, 523 F.3d at 945-46.

[127] *Id.* at 946.

[128] *Id.*

[129] *Id.* at 947.

[130] *Id.* at 948.

[131] *Id.*

> Amendment interest is also at stake. *See id.* at 506-08 (citing *New York v. P.J. Video*, 475 U.S. 868, 874 (1986) (refusing to require a higher standard of probable cause for warrant applications when expressive material is involved)).[132]

One can hear the doctrines locking into place or clashing, depending on one's view. The computer has become a "digital briefcase" of the twenty-first century.[133] This concern is reflected in an earlier Ninth Circuit case, *United States v. Romm*,[134] however there the court never discussed the routine versus non-routine nature of the computer search where the search included a computer forensic team that was able to recover deleted files and determine when the files were created, opened, or modified.[135] As speculated by one commentator, consider someone receiving an unsolicited, spam e-mailing containing illicit photos.[136] Even if deleted, a border search might reveal the message and it could be used against the individual in court, given the recent *Arnold* decision.[137]

As one would expect, speculation soon became reality; given technology, the border exception, and one's expectation of privacy, it was only a matter of time before a case arose. The next legal doctrine to be brought into play by the border jurisprudence is the Fifth Amendment, or the right against self-incrimination. Thus far, the closest case on point is *In Re*

---

[132] *Id.*

[133] *See* Michael Pellegrino, *International Business Travelers Beware*, ILL BUS L.J. (Feb. 22, 2008), *available at* http://iblsjournal.typepad.com/illinois_business_law_soc/2008/02/picture-yoursel.html (last visited Nov. 28, 2008).

[134] United States v. Romm, 455 F.3d 990 (9th Cir. 2006).

[135] *Id.* at 994-95.

[136] *See* Pellegrino, *supra* note 133.

[137] *See Arnold*, 523 F.3d at 947. The *Arnold* holding rejects the view that a search of a person's laptop implicates privacy and dignity interests. *Id.* In an earlier case, *United State v. Molina-Tarazon*, it was asserted that "government intrusions into the mind . . . are no less deserving of Fourth Amendment scrutiny than [physical intrusions]." 279 F.3d 709, 716 (9th Cir. 2002). The *Molina-Tarazon* court indicated that because of the vast amount of private thoughts and sensitive data that can be stored on data drives, searching them is analogous to searching the mind, and thus they implicate privacy and dignity interests. *Id.* at 716. Consequently, the court held searches of laptops and other electronic storage devices require reasonable suspicion. *Id.* at 717.

Boucher.[138] Sebastien Boucher was crossing the border from Canada to Vermont when border agents began to question him.[139] Agents saw a laptop in the back seat of his car and opened it up.[140] His computer was not password-protected; an agent began to look through it.[141] The agent came across 40,000 image files with titles that strongly suggested the files themselves were child pornography.[142] For example, one file was labeled "2yo getting raped during a diaper change."[143] The files had been opened six days earlier, but the agent found that he could not open the file when he tried to do so.[144] Agents asked Boucher if there was child pornography in the computer, and Boucher said that he was not sure.[145] He downloaded a lot of pornography onto his computer, he said, but he deleted child pornography when he came across it.[146] Boucher then assisted the officer in accessing drive Z that contained preteen pornography.[147] The computer was seized and the agents made a mirror image of the drive, but when they tried to access the Z drive again, it was protected by "Pretty Good Privacy" (PGP) software, which encrypted, password-protected the material, and made it inaccessible.[148] A grand jury subpoenaed the password and Boucher pled the Fifth.[149]

Though both the government and Boucher agreed the "contents" of the computer were not protected by the Fifth Amendment, Boucher argued the "password" was testimonial, protected and privileged.[150] Fingerprints, blood samples and

[138] *In Re Boucher*, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).
[139] *Id.* at *1.
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] *Id.* at *2.
[148] *Id.*
[149] *Id.*
[150] *Id.*

voice recording are not protected under the Fifth Amendment.[151] As noted by the court in *Boucher,* the Supreme Court in *United States v. Hubbell*[152] reasoned that while a combination to a wall safe was testimonial and protected, surrendering a key to a strongbox was not.[153] The magistrate judge, Jerome J. Niedermeier, found that a password is more like a combination, since it is in the suspect's mind, it is not a "physical thing," it compels him to display the contents of his mind, and therefore must be protected:

> Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?" If Boucher does know the password, he would be faced with the forbidden trilemma; incriminate himself, lie under oath, or find himself in contempt of court.[154]

Critics of the case note that the government already knew that the files belonged to Boucher since the computer was in his car; the government was aware that he knew the relevant password partly because he assisted them in searching the Z drive; and Boucher admitted to downloading material during the interview.[155] Therefore, the alleged self-incrimination that follows from Boucher's revealing his password is simply the content of these other accessible computer files.[156] The government will not be forcing the defendant to let the officers know that he is linked to the computer files, the evidence will instead be the product of lawful investigation followed by a demand for a password that everyone already knew the

---

[151] *Id.* at *4.

[152] United States v. Hubbell, 530 U.S. 27, 43 (2000).

[153] *In Re Boucher*, 2007 WL 4246473 at *4.

[154] *Id.* at *4.

[155] *See* Sherry F. Colb, *Does the Fifth Amendment Protect the Refusal to Reveal Computer Passwords? In a Dubious Ruling, A Vermont Magistrate Judge Says Yes*, (Feb. 4, 2008), *available at* http://writ.news.findlaw.com/colb/20080204.html (last visited Nov. 28, 2008).

[156] *Id.*

defendant possessed.[157] What the defendant had to do, in other words, was surrender a password much like a key to a briefcase or a locked compartment inside a trunk. Under the critics' analysis the government could grant immunity for the password and then prosecute for the underlying contents of the files, and a refusal to provide the password would amount to contempt and possible incarceration.[158]

These facts are underscored by the Office of National Counterintelligence Executive's warning for those traveling abroad and what one can expect to encounter at border crossings. But in the *Boucher* case rather than national security issues it appears that criminal activity is what is at stake. Though Fourth Amendment protection is diminished at the border, for U.S. citizens in a non-national security case, is similarly the Fifth Amendment? Clearly one could not take a briefcase across the border and refuse to have its contents examined. Is a computer a digital briefcase without Fifth Amendment protection? Eventually the Supreme Court will have to address this question and resolve the clash of these doctrines—maybe.

III. CONCLUSION: TRADE-OFFS, BALANCING OR RESILIENCY?

Combating terrorism in the digital age has produced a clash of legal, political and social doctrines. Technology, theories of state power, the individualized nature of modern terrorism, and our legal traditions have clashed over the need for security. A threshold question for the public policy debate is whether or not one believes the threat of terrorism is an *existential* threat. For some, an existential threat is one that can only be posed by a competing state power with nuclear weapons; terrorism therefore is not such a threat. Terrorism is a form of "empire baiting" and must be countered with measured law enforcement approaches that respect our legal traditions and follow our civil

---

[157] *Id.*

[158] Declan McCullagh**,** *Judge: Man can't be forced to divulge encryption passphrase***,** (Dec. 14, 2007), *available at* http://news.cnet.com/8301-13578_3-9834495-38.html (last visited Nov. 28, 2008).

liberties. Any intrusive government measure must be balanced against how our freedoms or rights are diminished. This approach is more willing to accept risk at the expense of faux security since stopping all attacks is impossible. Additionally, this approach advocates more focus on resiliency, building infrastructure and redundancy in our system.

For others, a terrorist with one nuclear device or biological weapon poses a threat that justifies expansive executive powers and enhanced investigative tools to prevent any and all attacks, the key to prevention. Security or the chance to stop a terrorist is worth the diminution of certain rights or privileges. For this school of public policy, our security forces our people of good will who are making sacrifices to protect the republic: only those who have something to hide—terrorists, criminals and violators—should fear this new requirement of personal transparency. Government violations or infractions will be on the margin and prosecuted accordingly.

For those in the legal arena the clash becomes focused on specific cases involving specific property, or persons at specific locations—borders and computers—triggering specific articles and clauses of the Constitution—the Fourth Amendment, the Fifth Amendment, and separation of powers. As de Tocqueville pointed out in the early nineteenth century in *Democracy in America*, "[s]carcely any political question arises in the United States that is not resolved, sooner or later, into a judicial question."[159] The legal balancing requires an analysis of the inherent power of the President, congressional statutes and the power of particular rights in the context of the threat, since no right is absolute.

The Supreme Court jurisprudence in this area has shown significant deference to the sovereignty of the state to defend its territory at the diminution of Fourth Amendment protection. U.S. citizens and non-U.S. citizen travelers are treated alike and receive minimum protection when at the border. Computer technology and encryption are raising Fifth Amendment rights

[159] 1 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA, 280 (Phillips Bradley, ed., Alfred A. Knopf 1948) (1945).

in the face of states need to gather information for criminal and terrorist networking at ports of entry. Eventually the Court will be called on to balance these interests. The Court's border jurisprudence currently leans towards the state's need to protect.

Similarly, foreign borders, as the NCIX has warned, are potential Wild West frontiers whereby electronic data can be mirrored and monitored for the foreign state's advantage. The electronic frontier, from the perspective of the individual or business entity, is currently a hostile environment due to the state's fear of the potential for individualized attack and the state's need for critical information for advantage. The current jurisprudence has not been a safe port in the storm.

In the opening quotation of this article, Senator Feingold reasoned, "if the courts can't offer that protection, then that responsibility falls to the Congress."[160] Yet, Congress thus far has not legislated on border cases, and its performance in the FISA area has not satisfied too many: More study is required.[161]

---

[160] *See supra* note 1 and accompanying text.

[161] *See Restoring the Rule of Law: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary* (2008), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=3550&wit_id7415 (last visited Nov. 28, 2008) (testimony of Suzanne E. Spaulding, Principal, Bingham Consulting Group LLC). Spaulding suggests that the new administration should conduct a comprehensive review of domestic spying. *Id.* Some of the key issues that any comprehensive review should address include:

- A review of the Foreign Intelligence Surveillance Act, including changes enacted as part of the PATRIOT Act and in the amendments this summer, assessing both the statutory language and its implementation.
- The recent amendments focused on meeting a particular need asserted by the current Administration and, as noted earlier, many Member of Congress stated their view that it was a deeply flawed bill and should be re-visited in the coming session of Congress. Beyond that, however, what seemed lost in the debate is the need to reassess FISA more generally in light of the vastly higher level of international communications engaged in by Americans today, via the Internet as well as by phone, than was the case in 1978. Does it still adequately protect innocent Americans from unwarranted government intrusion into their private communications?
- In addition, the electronic and physical search provisions of FISA, complex from their inception, have become virtually impenetrable to nearly all but those who work with it on a daily basis—and perhaps even to those unfortunate souls! Is

Moreover, immigration law and anti-terrorist measures have become so entangled that America's historic ability to be a beacon for the world's talent has been called into question over our administration of the skilled visa program.[162]

The clash of doctrines has been a function of the difficulty of the problem set. Each institution, the executive, the legislature and the courts, has approached the interlocking propositions sketched out at the beginning of the article from each of its institutional competencies. The results thus far have been unsatisfactory from all policy perspectives. Science and technology have been the key engines to our prosperity and quality of life; while at the same time these disciplines have produced the existential threats that can end both.

The executive, the congress and the courts, are at the beginning of the regime of how to combat terrorism in the digital age. There is a clear need to forge new principles and norms to harmonize the din that is resulting from the clash.[163] More institutional reform is needed for the Intelligence Community (IC) and the law enforcement community. The creation of the

---

there a way to simplify this regime to ensure compliance, enhance the prospects for effective oversight, and improve public trust?

- This review should include careful consideration of the important role of judges. As Supreme Court Justice Powell wrote for the majority in the Keith case:

> The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

Id. at 4.

[162] See discussion of H1-B visas for skilled workers, whereby Microsoft was unable to acquire visas for a third of the foreign job candidates it required. EDWARD ALDEN, THE CLOSING OF THE AMERICAN BORDER: TERRORISM, IMMIGRATION AND SECURITY SINCE 9/11, 282 (2008).

[163] Concluding paragraphs drawn from Harvey Rishikof, *The "War on Terror" and Prevention: Improving the Domestic Paradigm for the Digital Age*, 17 THE NAT'L STRATEGY FORUM REV. 1, *available at* http://www.nationalstrategy.com/Programs/NationalStrategyForumReview/PastNSFRIssues/Winter2007NSFRV171/tabid/112/Default.aspx (last visited Nov. 28, 2008).

Director of National Intelligence has not resulted in the coordination for which many had hoped. The need for better collection, analysis and dissemination of information still plagues the IC. In addition, better delineation of the role of military intelligence and its relation to its civilian counterparts requires more analysis and connectivity. A National Commission is required to draw on expertise from both sides of the political aisle, the private sector and the legal defense bar to craft a long-term reform package to balance the equities of the parties involved in prosecuting the War on Terror.

Second, the debate over executive authority and congressional reticence must come to an end. The assertions of presidential authority excluding Congress and barring Congress from helping to shape and structure surveillance programs have helped generate unnecessary suspicion and rancor. A way must be fashioned to generate a better working relationship between Congress and the Oval Office. There must be adequate due process protections built into reforms to satisfy traditional concerns of privacy, the current FISA reforms need to be revisited.

Third, the judiciary must be part of the review process whenever surveillance of U.S. or non-U.S. parties is involved**.** As the government increasingly relies on the private sector to gather data, and then uses this data forever increasing sophisticated data mining, judicial supervision should be part of the process. As more intrusive technological tools become available, reform packages must include more resources for robust Inspector General investigations. Current border jurisprudence enhances the need for a national security court with expedited procedures for review and concentrated expertise in due process, as had been done in civil law countries.[164]

Fourth, given the nature of globalization, the digital world and borders, a more international approach is required to address the issues. This enterprise will have to address the

[164] *See* Harvey Rishikof, A FEDERAL TERRORISM COURT**,** PPI, Nov. 14, 2007, *available at* http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=124&subsecID=307&contentID=254507 (last visited Nov. 28, 2008).

issue of *Weberian* sovereignty head on. What are the limits to the State's ability to have access to electronic data, and what will be the international penalties for violating such norms? This is a tough issue, but avoidance is not the answer.

This will be the challenge for our generation, but it is a challenge we must meet because too much is at stake. How we treat borders and data will define the power of the state and privacy in the twenty-first century.