NATIONAL SECURITY LAW REPORT
Standing Committee on Law and National Security
AMERICAN BAR ASSOCIATION
VOLUME 32, NUMBER 1
WINTER 2010

Table of Contents

Gregory S. McNeal
Editor
gregory.mcneal@pepperdine.edu

A Comparative Look at The Investigative Detention of Terrorist Suspects in The United States, The United Kingdom and France

By Dan E. Stigall, U.S. Department of Justice, author of Counterterrorism and the Comparative Law of Investigative Detention (Cambria 2009). Opinions expressed by the author are personal and not attributable to any government agency.

The practice of investigative detention is, at least in theory, anathema to U.S. criminal law. A review of U.S. jurisprudence reveals dire warnings of the dangers of detaining a person for purely investigative purposes. But is the practice of investigative detention truly incompatible with a liberal democracy? Such questions seem worthy of exploration given that the practice of questioning and examining a source to obtain the maximum amount of usable, reliable information in the least amount of time is a fundamental element of counterterrorism. This is true, not only for intelligence gathering purposes, but for law enforcement agencies, which must complete an investigation and attain enough evidence to convict a suspect, disrupt ongoing terrorist operations, and avert further attacks.

At the outset, it is probably beneficial to state what this article (and my book length treatment of the same topic) does not deal with. I do not conduct a detailed exploration of preventive detention mechanisms. To the contrary, my focus is a narrow one, dealing with the concept of investigative detention of terrorism suspects and outlining the investigative detention powers of the United States, the United Kingdom, and France. The comparators I chose for the study are useful, in my view, because they are widely regarded as liberal democracies with fair criminal justice systems. Moreover, both are considered true democracies in which the citizens enjoy a generous amount of freedom and protection from government intrusion. Furthermore and quite importantly both the U.K. and France have had long experiences with terrorism and have made adjustments to their domestic criminal laws in order to counter that threat. A study of those systems, therefore, provides greater understanding of the powers available to law enforcement in those countries (for joint international operations that involve domestic law enforcement entities) and allows policy-makers to explore the possibility that the tools enacted in democracies across the Atlantic could be somehow mimicked—or could provide inspiration—here at home.

My proposals are not intended to displace other arguments such as those who call for a special terrorist court, possible preventive detention mechanisms, special tribunals, etc. My proposals are somewhat distinct from those arguments (though obviously related).

Continued on **page 2**

Investigative Detention, from page 1

I, instead, seek to demonstrate how other countries have used their ordinary criminal processes for counterterrorism purposes and how U.S. criminal law can be better attuned to the problem of terrorism. I further seek to demonstrate that issues of terrorist detention do not necessarily require the utter abandonment of our criminal model. To some extent, the analysis of U.S. law which I explore in greater detail in the book, calls into doubt the frequent and blanket assertions regarding the fundamental incompatibility of investigative detention with the U.S. legal system especially when taking into account much of the legal maneuvering in post–September 11 America. But a comparative analysis allows us to question such assertions in broader scope. This is because a review of the legislative responses of the United States, the United Kingdom, and France demonstrates that the ability to detain terrorists and interrogate suspects has been central to each country's counterterrorism effort. Otherwise stated, there are grounds for asserting that investigative detention rather than being anathema to liberal democracy has been, in fact, a hallmark of the responses of liberal democracies to significant security issues such as terrorism. For instance, when one looks at the power to initially stop suspects in Europe, one sees greater powers afforded police in counterterrorism cases. In the United Kingdom a terrorist suspect can be stopped and searched by the police based on mere suspicion that the person is a terrorist, in order to discover whether he or she has possession of anything that may constitute evidence that he or she is a terrorist. Should any evidence that was obtained in the course of that stop and search (or any evidence independent of that event) give rise to the mere suspicion that a person is a terrorist, the suspect may then be arrested. Likewise, across the Channel in France, the procedures for *contrôle d'identité* allow that a person may be stopped and his or her identity verified based solely upon suspicion of a potential breach of public order. This initial contact with police through a *contrôle d'identité* can easily lead to the discovery of a criminal offense. Thus, one sees in the investigative detention regimes of both the United Kingdom and France a degree of permissiveness that makes detaining terrorist suspects easier.

"There are grounds for asserting that investigative detention rather than being anathema to liberal democracy has been, in fact, a hallmark of the responses of liberal democracies to significant security issues such as terrorism."

Beyond the initial stop, the differences in the allowable mechanisms for investigative detention become even more evident. In the United Kingdom, after being stopped, the terrorist suspect may be detained without charge for twenty-eight days from the time of arrest purely for investigative purposes—during which time the police may conduct an investigation while holding the suspect safely under their guard. French counterterrorism legislation, likewise, allows police to place any suspect in a form of detention known as *garde à vue* for six days held without charge and subject to interrogation without the presence of an attorney. At that point, French police have the power to detain a witness for a prolonged period during the preliminary phase of the investigation, without ever charging the individual, before turning over the suspect to the judicial police. Thereafter, for the necessity of the investigation or for reasons of security, a person can be placed in what is known as *détention provisoire*. For cases involving serious offenses, such as terrorism, a person may be kept in *détention provisoire* for up to three years and up to four years if the offense took place outside of French territory.

Of course, each of these legal regimes affords certain rights to terrorist suspects – but those rights are diminished due to the nature of the threat posed by terrorism. For instance, during the interrogation process, U.K. legislation grants such suspects the right to a legal advisor, but this right can be suspended for up to forty-eight hours and, when it is allowed, it can be ordered that a detained suspect is only to receive legal advice in the sight

and hearing of a police officer. In France, similarly, an individual in *garde à vue* under normal circumstances only has a right to consult with an attorney at the very beginning of the period of detention and then again, in cases of prolongation, after the twenty-fourth hour of detention. In cases of terrorism and narcotrafficking, however, the individual may not consult with an attorney until the seventy-second hour (after the second prolongation of detention). Further, criminal suspects in France do not have to be informed of their right to remain silent. In both the United Kingdom and France, therefore, terrorist suspects have diminished legal protections while in custody granting investigators greater access to them and increasing the ability of investigators to conduct interrogations.

U.S. law is also more permissive of investigative stops in situations where national security is concerned. The United States, of course, has its own mechanisms of de facto (if not de jure) investigative detention. Much has been written in recent years on the use of the Material Witness Statute, which allows the government to detain a person in connection with a criminal proceeding if it can demonstrate that the person (1) has information which is material to a criminal matter and (2) is a risk of flight. Such a warrant can be obtained through a showing that, based on probable cause, the witness in question has material information relevant to a criminal matter and his or her presence cannot be obtained through a subpoena. This standard is obviously different from the standard for arresting a criminal suspect in that law enforcement need not establish probable cause that the individual actually committed a crime – only probable cause that the person has information about a crime. This makes the inquiry more abstract and epistemological in nature. Courts have even upheld the use of this statute to hold potential witnesses for testimony before a grand jury.

In spite of the flexibility of that statute, however, there are significant limitations under U.S. law that apply even to detain Material Witnesses that serve to diminish investigative detention capabilities. For instance, in the United States, as every American attorney should know, the Fifth Amendment to the U.S. Constitution gives every suspect in custodial interrogation the right to remain silent, and, in order to ensure the free exercise of this right, if a person in custody is to be subjected to questioning, he or she must first be informed by the police (in clear and unequivocal language) that he or she has the right to remain silent. The cautionary warning must be accompanied by the explanation that anything said to investigators can and will be used against the suspect in court. Similarly, suspects in the United States have the right to consult with a lawyer and to have a lawyer present during interrogation. The moment a suspect requests a lawyer, the interrogation ends. Such rights are afforded to all criminal suspects no matter the suspected crime. Even noncitizens (against whom U.S. law enforcement seeks to bring criminal action) are afforded such protections.

"U.S. law is also more permissive of investigative stops in situations where national security is concerned."

This robust set of rights and privileges marks an obvious departure from the United Kingdom, which allows adverse inferences to be drawn from one's silence and allows suspension of one's right to an attorney for up to forty-eight hours. In addition, the adherence to such a rights-based system differs significantly from the French system, which does not require a suspect to be advised of his or her right to remain silent and allows only intermittent consultation with an attorney.

There are other areas of U.S. law that are worthy of note. Aside from the Material Witness Statute, the Omnibus Crime Control and Safe Streets Act carved out a "safe harbor" period that protects the admissibility of those statements made during a six-hour delay prior to bringing an arrestee before a magistrate, thus making it permissible to delay presentment to a magistrate for at least six hours. This can be viewed as a legitimate six-hour investigative period, albeit one that is obviously far shorter than that granted to investigators in the United Kingdom and France. There is no law in place allowing for its pro longation in cases involving national security or other exigencies.

Such comparisons form what I hope is an in-

Continued on **page 4**

Investigative Detention, from page 3

teresting exploration of the concept of investigative detention as it exists in the United States and in other democracies which are largely considered "free" and where human rights are safeguarded. In addition, the book aims to identify those areas of U.S. law that could be modified to grant U.S. law enforcement agents greater investigative powers in cases of suspected terrorism. I maintain that there is, drifting in the legal ether, enough material for the prudent legislator to grasp and sculpt a workable (if extremely limited) investigative detention scheme in the United States, primarily through the following five legislative changes: (1) enhancement of the ability of police to conduct "stop and frisks" though the enactment of law criminalizing membership in terrorist organizations; (2) the creation of a federal "stop and identify" statute; (3) maximization of the "public safety" doctrine; (4) doubling the six-hour "safe harbor zone" created in the Omnibus Crime Control and Safe Streets Act; and (5) enacting a civil detention law such as that proposed by Professor Tung Yin. While this, of course, is not an endeavor that should be undertaken lightly, such changes are worth considering given recent omens in the jurisprudence which portend an uncertain future for the Material Witness Statute as an investigative detention mechanism. *See, e.g. al-Kidd v. Ashcroft*, 580 F.3d 949, 963 (9th Cir. 2009) (holding that "when a prosecutor seeks a material witness warrant in order to investigate or preemptively detain a suspect, rather than to secure his testimony at another's trial, the prosecutor is entitled at most to qualified, rather than absolute, immunity.")

The measures proposed in my book may rightly be criticized as pushing the envelope of existing law, but it must be recalled that U.S. jurisprudence has traditionally allowed a certain degree of elasticity when national security concerns are implicated and specifically where terrorism is concerned. Even then, as the book emphasizes, the counterterrorism capabilities my proposals would create in U.S. law would still fall short of the robust investigative detention regimes that exist across the Atlantic. Nonetheless, they would provide U.S. law enforcement authorities with useful tools within the framework of the existing criminal law system by which terrorist suspects across the spectrum (citizen or noncitizen) could be lawfully detained and investigated. While this is not an endeavor to be lightly undertaken, I contend that the nature of the threat posed by terrorism requires a hard and honest look at what police powers are actually needed and how such powers can be within a normalized legal framework as they are in other legal systems. ■

The Problem With Law Avoidance

By Geoffrey S. Corn, Associate Professor of Law, South Texas College of Law

It's been nearly 10 years since United States initiated what President Bush characterized as the Global War on Terror. Although that characterization has been abandoned by President Obama, there is no indication that the new President intends to abandon the use of military power as a means to disrupt or disable the capabilities of transnational terrorists. Operatives associated with al Qaeda continue to be detained preventively, targeted with military force both in and outside of Afghanistan, and killed as a measure of first resort. Much to the chagrin of many supporters of candidate Obama, his Department of Justice continues to defend these policies in federal courts.

The recent federal court decision in *Al-Bihani v. Obama* has triggered significant controversy related to the role international law plays in defining the authority to continue to engage in these practices.

Distinct from the courts dismissal of *Bihani's* substantive arguments, the court's assertion that it need not consider international law when interpreting the scope of authority provided by Congress for the prosecution of the struggle against transnational terrorism has been widely condemned. But this opinion is just the latest manifestation of the difficulty in defining the limits of that authority for a struggle that falls in a twilight zone between war and peace, conflict and law en-

forcement. This decision has once again brought to the forefront of the legal debate the struggle against transnational terrorism and how that characterization influences authorities and obligations related to prosecuting that struggle.

One aspect of the debate related to this struggle is unquestionably clear: the nature of military operations directed against transnational terrorism failed to fit neatly within the existing law triggering framework. As I've written elsewhere, this framework, based on common articles 2 and 3 of the 1949 Geneva Conventions, was never understood as addressing and accounting for the possibility of an armed conflict between the state and nonstate entity occurring outside the territory of the state. This led to substantial uncertainty following the initiation of military operations against al Qaeda in the months following the terrorist attacks of September 11, 2001. Multiple theories were proffered to address the law application dilemma created by these operations. On one end of the spectrum was the argument that the struggle against al Qaeda was a pure law enforcement endeavor with no basis to assert authority derived from the law of armed conflict. On the other end of the spectrum was the theory central to the initial policies of the Bush administration: anyone determined by the President to be sufficiently associated with al Qaeda could be detained as an unlawful enemy combatant by virtue of the existence of an armed conflict. In between these two extremes were other theories: the struggle against al Qaeda was an "internationalized" common article 3 conflict; a strict interpretation of articles 2 and 3 that drew a sharp distinction between al Qaeda operatives captured in Afghanistan, who could only be detained as militia groups associated with the Taliban, and those captured elsewhere, who were international criminals not subject to armed conflict based preventive detention; and the theory that I have offered in several articles, that the armed component of this struggle is best understood as a "transnational" armed conflict triggering fundamental principles of the customary law of armed conflict.

For the U.S. armed forces, this legal debate became increasingly irrelevant as each branch of the United States government accepted the proposition that at least certain components of the struggle against transnational terrorism qualify as armed conflicts. Implicit within this characterization was the understanding that the authority and obligations in relation to this struggle would be derived from the law of armed conflict. While there was some uncertainty related to the obligation prong of this equation resulting from the initial legal interpretations of the Bush administration Department of Justice, that uncertainty seemed eliminated with the Supreme Court's decision in *Hamdan v. Rumsfeld*, a decision based on the conclusion that all armed conflicts trigger basic humanitarian obligations.

The District of Columbia Court of Appeals in *Al-Bihani v. Obama* concluded that the war making provided by the AUMF and other statutes may be enhanced, but never limited by the law of armed conflict ("Therefore, while the international laws of war are helpful to courts when identifying the general set of war powers to which the AUMF speaks, *see Hamdi*, 542 U.S. at 520, their lack of controlling legal force and firm definition render their use both inapposite and inadvisable when courts seek to determine the limits of the President's war powers." *Al-Bihani v. Obama*, 2010 U.S. App. LEXIS 102 (D.C. Cir., Jan. 5, 2010) at *10). This conclusion risks the creation of an entirely new front in the debate over the appropriate regulatory framework to govern this struggle. It is unfortunate that the court ignored centuries of jurisprudence on the relationship between domestic authority to wage war and the *jus belli*. However, what is even more unfortunate is that this opinion also ignores the necessity to engage in the type of careful and deliberate analysis of where the line between armed

"One aspect of the debate related to this struggle is unquestionably clear: the nature of military operations directed against transnational terrorism failed to fit neatly within the existing law triggering framework."

Continued on **page 6**

Law Avoidance, from page 5

conflict in law enforcement begins and ends, and what rules derived from the law of armed conflict should be applied to the struggle against transnational terrorism when actions fall on the military conflict side of the divide.

In response to this decision, Al Bihani sought *en banc* review. Although the government opposed such review, it also emphasized its disagreement with the interpretation of the role of the *jus belli* adopted by the Al Bihani panel. According to the government brief in opposition to the request for *en banc* review:

Petitioner cites the panel majority's statement that the "premise that the war powers granted by the [. . . (AUMF)] and other statutes are limited by the international laws of war * * * is mistaken." The Government agrees that this broad statement does not properly reflect the state of the law. The Government interprets the detention authority permitted under the AUMF, as informed by the laws of war. That interpretation is consistent with the Supreme Court's decision in *Hamdi v. Rumsfeld*, and with longstanding Supreme Court precedent that statutes should be construed as consistent with applicable international law. (*Al-Bihani v. Obama*, Case No. 09-5051 (May 13, 2010), Government Response to Petition for Rehearing and Rehearing *en banc)*.

"Judge Brown emphasized this lack of relevance of the customary international laws of war..."

On August 13, 2010, the D.C. Circuit Court of Appeals rejected Al Bihani's request, in an opinion that included seven concurrences. The court emphatically endorsed the original panel's rejection of customary international law as a source of constraint on the government's execution of war powers. In his lead opinion, Judge Brown emphasized this lack of relevance of the customary international laws of war, and went even further by noting that there was nothing inherently illogical in Congress authorizing deviations from the customary laws of war in response to the type of unconventional threat the United States found itself engaged against. (*Al-Bihani v. Obama*, Case No. 1:05-cv-01312 (August 31, 2010), On Petition for Rehearing En Banc, (Brown, J., concurring)).

In his concurring opinion, Judge Kavanaugh concluded that nothing in the AUMF indicated Congress intended to incorporate customary international law norms into the grant of authority to the President to wage war against al Qaeda. As a result, the court had no basis to conclude that the AUMF's grant of authority for the President to use "necessary and appropriate" force is in any way limited by the laws of war. Nor, according to Judge Kavanaugh, do the Geneva Conventions impose any limitations on the President (at least judicially enforceable limitations), because these four treaties are non-self executing. Finally, in a footnote Judge Kavanaugh concludes that even if international law in the form of a non-self-executing treaty or customary norms were judicially enforceable in theory, relief for Al Bihani would still be foreclosed because Congress' definition of detainability trumped those sources of law. (*Al-Bihani v. Obama*, Case No. 1:05-cv-01312 (August 31, 2010), On Petition for Rehearing En Banc, (Kavanaugh, J., concurring)).

Unless the Supreme Court chooses to review the Al Bihani decision, this rejection of customary international law as a judicially enforceable source of authority for defining the scope of legitimate detentions will control all subsequent habeas challenges in the D.C. Circuit. This may facilitate judicial review of habeas challenges, but it unfortunately fails to comport with the longstanding U.S. understanding of the relationship between domestic authority to wage war and the *jus belli* as a source of both authority and obligation during war.

I have proposed previously that one method to determine the locus of this boundary is to analyze the nature of the authority invoked by the government in response to a terrorist threat. More specifically, I have argued government authorization to engage terrorist enemies pursuing the rules of engagement that authorized the use of deadly force based solely on the determination of status-an authority that implicitly invokes the principle of military objective-indicates the existence of armed conflict. I concede that this is not

a perfect test, but I believe that because it is linked to the nature of the authority being invoked by the state, it provides an effective insight into the true nature of the operations. When those operations take on the character of armed conflict because the armed forces are authorized to employ combat power as a measure of first resort against a defined enemy based on the determination of status, and those operations must be regulated by complementary principles derived from the law of armed conflict. But even accepting the efficacy of this test for determining when the law of armed conflict is triggered only begins to resolve the type of questions raised in the *Al Bihani* case, questions related to the rules triggered by such a situation, and how to determine when such conflicts terminate.

By avoiding analysis of the difficult question of whether the law of armed conflict authorized Al Bihani's preventive detention, whether that authority continues, and the conditions that will terminate that authority, the court has set the conditions for avoiding future avoidance of similar complex yet critical questions. If, as is apparent from the positions staked out by the Obama administration, the United States will continue to implicitly if not explicitly rely on the characterization of this struggle in armed conflict as a basis to justify its treatment of suspected terrorists, what is really necessary is analysis of the scope of authority and obligations derived from the law of armed conflict that apply to this struggle, not judicial avoidance.

The Al Bihani case was in many ways an ideal opportunity to engage in such analysis. One issue that is particularly significant in relation to detainees like Al Bihani is the question of how the law of armed conflict defines the process by which nonstate belligerents sufficiently disassociate themselves from the groups that they ostensibly associated with in the context of an armed conflict, and how that disassociation impacts authority to initiate and continue preventive detention based on the principle of military necessity? It is clear that unlike a traditional interstate armed conflict, individuals detained by virtue of their connection to a nonstate group engaged in a transnational armed conflict will never be able to claim the protection of the GPW. Accordingly, the provision of that treaty that requires repatriation at the termination of hostilities is ineffective to address the issue of detention termination. In fact, the law of non-international armed conflict is virtually silent on repatriation obligations (the only reference that even comes close to addressing the issue in Additional Protocol II is a requirement that parties be generous when considering granting amnesty to individuals who have been detained in the context of a non-international armed conflict). But does this mean that there are no rules or principles to be derived from the law of armed conflict that offer guidance or parameters in relation to the question of when detention should terminate?

"...the law of non-international armed conflict is virtually silent on repatriation obligations"

My transnational armed conflict jurisprudence has been criticized as an unjustified endorsement of an invalid theory of invoking the authority of the law of armed conflict. Ironically, the motivation for that scholarship was always an attempt to establish a framework that would prevent the government from invoking authority while at the same time disavowing any obligation derived from the law that purportedly provides such authority. In short, my ROE trigger concept was intended to ensure that in the future it would be impossible to disavow obligations derived from the law of armed conflict when the United States authorized the use of military force that implicitly invokes the principle of military objective. Implicit within this theory is that states engaged in such transnational armed conflicts must consider not only the principles of the law that grant them authority to kill, capture, and detain their enemies, but also principles that operate to protect the fundamental humanitarian interests of these objects of state action.

By avoiding the law applicability issue, the DC Circuit Court has resurrected the troubling prospect of an authority without legal framework. As the Supreme Court noted in its *Hamdi v.*

Continued on **page 8**

Law Avoidance, from page 7

Rumsfeld decision, the authorization to use all necessary means against the terrorist threat by implication invoked the principle of military necessity. Accordingly, I have always understood that opinion to indicate that preventive detention related to hostilities against individuals and entities falling under the umbrella of that authorization was justified pursuant to the principle of military necessity. If this is true, it begs the question of why other principles of the law of armed conflict - principles that may in fact operate to protect the interests of these detainees - are not equally applicable by operation of this same authorization.

One such principle that a more reasoned analysis of the relationship between the AUMF and the law of armed conflict might have implicated is a principle of repatriation. Whether derived from an analysis of the principle of military necessity (repatriation would be required when the facts indicated preventive detention was no longer necessary), the principle of humanity (establishing a mechanism to ensure that individuals are released from preventive detention when the nature of the conflict in which they were captured can no longer support continued detention), analogy to the repatriation provision of the GPW, or a combination of all of these factors, it is logical that the law of armed conflict could be interpreted as establishing some endpoint in the detention of even nonstate belligerents. This could also include analysis of how nonstate belligerents could effectively disassociate themselves from the objectives of an organization in a manner sufficient to justify the termination of detention.

Instead of analyzing the applicability of the law of armed conflict as a potential source of authority and obligation in relation to Al Bihani's initial and continued preventive detention, and how that law should evolve to deal with the unique challenges associated with individuals like Al Bihani, the DC Circuit Court invoked a questionable theory of statutory interpretation to avoid these difficult questions.

This avoidance is problematic on a number of levels, and as noted above has already triggered substantial criticism as a manifestation of disrespect for international law, and a failure to adhere to long-standing principles of interpreting domestic statutes that implicate international law. This avoidance also forgoes an opportunity to address a number of critical issues related to how the law of armed conflict impacts the authority to preventively detained nonstate belligerents. But what is most problematic about this avoidance is that it suggests a resurrection of a theory of authority without obligation that utterly distorts the fundamental balance that lies at the very core of the law of armed conflict, a distortion that is ultimately contrary to the interests of our nation and our armed forces. ■

A Response To Geoffrey Corn

By, Laurie Blank, Acting Director, International Humanitarian Law Clinic, Emory Law School

I share Professor Corn's concern about the problem of law avoidance hovering beneath the surface of the D.C. Circuit Court's opinion in *Al-Bihani*. The dangers inherent in seeing the law as a source of authority but not a corresponding source of obligation are particularly significant when military force is involved. The very nature of the law of armed conflict – which balances military necessity and humanity – is a balancing of authority and obligation. With the right to use force as a first resort must come concomitant obligations to use that force in accordance with the law, both in terms of the conduct of hostilities and the treatment of persons within the zone of combat.

As Professor Corn has written elsewhere, the drafters of the Geneva Conventions specifically targeted the problem of law avoidance in creating the framework for triggering the law of armed conflict. Whereas once countries have denied *jus in bello* obligations by claiming that they were

not engaged in "war", a term with specific legal connotations, the Geneva Conventions eliminated that particular circumlocution by creating a trigger for law applicability based on the existence of an armed conflict.

In response to the post-9/11 problem of classifying an armed conflict between a state and a transnational non-state entity occurring outside the territory of that state – a problem that led to the very law avoidance apparent in the *Al-Bihani* decision – Professor Corn has suggested, as he explains here, that an appropriate trigger should be the nature of the authority the state invokes, in particular as represented in the rules of engagement (ROE). As such, ROE authorizing targeting based on status alone – meaning that all members of the enemy armed forces are legitimate targets based on that status alone – would trigger the laws of armed conflict. ROE authorizing targeting based on conduct – meaning that an individualized analysis of the threat a potential target poses – would not trigger the laws of armed conflict.

This proposal is extremely helpful in one significant way: it patches the loophole some see in the existing Geneva Conventions common article 2 and common article 3 framework of international and non-international armed conflict and opens the door for application of the law of armed conflict to what many now refer to "transnational armed conflict."

But relying on ROE analysis as the trigger for law applicability raises an equally significant problem. States will have a strong motivation to issue status-based ROE so as to use the authority inherent in the law of armed conflict – the right to use force as a *first* resort. When the law of armed conflict does not apply, domestic law and international human rights law apply, a much more restrictive framework for the use of force, marked primarily by the use of force as a *last* resort. To the extent a state can define its enemy by status, it will therefore seek to do so.

The danger here lies in the risk this approach poses for the principle of distinction, which I outline in my piece above. Where those who can only be identified as a threat through their conduct (civilians participating in hostilities is a classic example) are instead designated as targets based on a more generalized status determination, the state is no longer fulfilling its obligation to distinguish between those who are fighting and those who are not.

The result is that in seeking to eliminate one form of law avoidance, the notion of an ROE-based trigger raises another – rather than seeking to claim there is no armed conflict in order to avoid the obligations of the law (the law avoidance inherent in *Al-Bihani*), a state may seek overly broad characterizations of the enemy in order to reap the benefits of the authority in the law of armed conflict.

We should not simply reject Professor Corn's approach as dangerous, however, because it offers a valuable framework in which to view the nature of military operations against terrorists and other non-state entities. Rather, my goal would be to focus on the particular law avoidance problem it raises. Can we still use the status vs. conduct framework but somehow divorce the analysis from the state's invocation of authority, much like the drafters of the Geneva Conventions sought to do with the law avoidance problem of their time?

Perhaps the answer is to look to a combination of how the state views the enemy as reflected in the ROE *and* how the enemy views itself, as reflected in its composition and behavior. When both point to a status-based analysis, the law of armed conflict framework is clearly appropriate. When both point to a conduct-based approach, the law enforcement/human rights approach will carry more weight. We will still be left with the complicated questions in the middle, but perhaps we will have at least weakened the opportunities for law avoidance. ■

In Counterterrorism, the Law of War Is a Key Source of Law for the Courts

By Laurie Blank

In *Al-Bihani v. Obama*, the D.C. Circuit Court of Appeals stated that "the premise that the war powers granted by the AUMF and other statutes are limited by the international laws of war . . . is mistaken." Al-Bihani v. Obama, 2010 U.S. App. LEXIS 102 (D.C. Cir., Jan. 5, 2010) at *9. The Court continued, declaring that "the international laws of war [are] not a source of authority for U.S. courts." Id. With these statements, the Court seems to resurrect earlier claims that the Geneva Conventions are "quaint" or "obsolete."

Ghaleb Nasser al-Bihani was a cook in a paramilitary unit affiliated with the Taliban in Afghanistan. After his unit surrendered to the Northern Alliance in the fall of 2001, he was transferred to U.S. custody and has been held in Guantanamo since 2002. Unlike many other detainees at Guantanamo, al-Bihani was captured on the battlefield. So why would the law of war not be relevant?

Many who claim that the law of war, also called the law of armed conflict or international humanitarian law, is not a source of authority for U.S. courts contend that the conflict with the Taliban and with Al Qaeda in Afghanistan is a new kind of war, with a new kind of enemy. In this new war, they argue, the old rules of international law are too antiquated and should no longer apply. *Al-Bihani*, 2010 U.S. App. LEXIS 102 at *43-44 (J. Brown, concurring opinion).

In response, we should first remember that the U.S. Supreme Court stated in *Hamdi v. Rumsfeld* that the law of war informs its decisions regarding detention under the AUMF. The D.C. Circuit seems to disregard this holding in *al-Bihani*. Apart from the legal precedent supporting reliance on law of war principles, however, there are straightforward practical reasons that are important to consider as well.

We are in a new kind of war. Where once nations fought nations, now we fight insurgents, shadowy terrorist groups and other non-state entities. Where we once measured combat by the number of tanks or fighter jets destroyed, now we count roadside bombs and suicide bombers.

But does this new kind of war necessarily demand new rules? Does it mean that our courts should not rely on the law of war to reach decisions about persons captured and detained in the course of this new kind of war? Those who say yes point to the fact that the Geneva Conventions entered into force in 1949, only four years after World War II – ancient history in terms of the nature of conflict. However, the law of war and the fundamental principles it protects and promotes are in fact more critical than ever in light of the changing nature of conflict.

The Geneva Conventions, and the law of war for centuries before that, are based on four key principles: distinction, proportionality, military necessity and humanity. These principles form the foundation of our domestic law of war as well, as set forth in Army Field Manual 27-10, *The Law of Land Warfare*, and other service manuals.

The principle of distinction requires all parties in a conflict to distinguish between those who are fighting and those who are not and only target the former when launching attacks. It also requires those who are fighting to distinguish themselves from innocent civilians. Distinction has a simple but noble purpose – to protect innocent civilians from unnecessary suffering during conflict. It also protects soldiers by helping them understand whether persons they encounter are hostile or innocent.

The principle of proportionality seeks to balance military goals with protection of civilians. It prohibits an attack when the expected civilian casualties will be excessive compared to the anticipated military advantage. In essence, a commander must believe that the stated military goal is reasonable in light of any foreseeable incidental civilian casualties.

Military necessity recognizes that the goal of war is the complete submission of the enemy as quickly as possible and allows any force necessary to achieve that goal as long as not forbidden by the law. Destroying enemy capabilities is legitimate, therefore; wanton killing and destruction is not.

Humanity aims to minimizing suffering in armed conflict. To that end, the infliction of suffering or destruction not necessary for legitimate military purposes is forbidden. This principle stems from the code of chivalry, itself an early manifestation of the laws of war.

In today's conflicts, the U.S. and its allies often face enemies who deliberately attack civilians; who fight in civilian clothing so as to be able to blend into the civilian population for purposes of disguise and safety; and who use hospitals, mosques and schools as command posts and munitions storage depots. These complexities certainly complicate the application of the law during combat situations and make conflict ever more deadly for innocent civilians and soldiers alike.

Rather than suggest that the law of war cannot apply to new warfare and is therefore of no consequence, however, the nature of these contemporary conflicts demands exactly the opposite conclusion. As the International Court of Justice stated in the *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, new means of combat do not call the longstanding principles of the law of war into question. Existing codifications and applications of the laws of war may prove difficult to implement, but the fundamental principles detailed above remain as important as – if not more important than – ever *precisely* because of the increased danger to participants and non-participants alike.

Those who argue that we need new rules for these new wars must consider exactly which of these principles we no longer want or need and the impact of such a decision on both our troops and innocent civilians, who depend on the law of war for critical protections. I doubt that we so anxious to kill terrorists and jihadists that we are willing to disregard the need to figure out whether our targets are in fact terrorists before we shoot, or that we are willing to destroy as many villages as it takes to get that one elusive insurgent.

Instead, we should focus on making the law work better in unpredictable and difficult circumstances. For example, we need to sharpen our ability to differentiate between friend and foe so that we know who is dangerous and who to protect. Our enemies may not wear uniforms, but that does not give us the right to shoot innocents in their stead. Doing so is not just good law – it is good policy for operational reasons as well.

We need to examine how to better protect civilians caught up in the zone of combat while still enabling effective military operations. When insurgents seek shelter in local villages, we cannot simply choose between bombing the whole village or letting the insurgents walk free for fear of civilian casualties, but need to develop operational tactics that enable more surgical strikes.

We need to learn more about how insurgents and terrorists operate so we can target their facilities while still protecting civilian buildings and infrastructure. The fact that our enemies make roadside bombs in residential basements and store munitions in mosques or hospitals does not excuse our obligation to distinguish between military and civilian objects. Nor does it make this obligation obsolete. Rather, it means that we must marry a more discerning analysis of when a building becomes a legitimate target with more sophisticated intelligence information.

Finally, we must remember the role of humanity in war. Although it may sound incongruous in talking about conflict, which is naturally replete with killing, destruction and other forms of violence, the obligation to accord humane treatment to civilians and all those *hors de combat* – those who are not fighting, whether because of sickness, wounds or detention – is fundamental not just to the Geneva Conventions, but to the international and domestic law of war long before 1949.

Our courts can play an important role in reinforcing these fundamental principles and should use them as a source for decision-making. The key principles of the international law of war are sound and timeless in their purpose – rather than letting the challenges of new wars define us, we can use the law to rise to the challenge. ■

A Response To Laurie Blank

By, Geoffrey S. Corn

I share Professor Blank's criticism of the approach adopted by the DC Circuit Court of Appeals. In my view, the nation and our armed forces would be far better served by a careful and legitimate analysis of whether the law of armed conflict applies to Al Bihani's situation and how the principles of that law define the scope of government authority for his continued preventive detention. Instead, the court simply avoids all these difficult questions by asserting that it need not consider the influence of the *jus belli* because Al Bihani's detention was authorized by Congress through the AUMF and other statutes. Professor Blank has already exposed how this interpretation of the statute appears inconsistent with the Supreme Court's decision in *Hamdi v. Rumsfeld.* What strikes me is that it is also inconsistent with the way in which courts in this country have interpreted the relationship between domestic authority to wage war and the law of war since inception of the Republic.

As far back as the quasi war with France our courts have recognized that when the nation is engaged in war, be it war *de facto* or war *de jure*, the *jus belli* is inextricably linked with the authority of the nation. In *Bas v. Tingy*, the Supreme Court taught us that while it is true that Congress can set limits on the scope of war, it is the *jus belli* that defines the nature of authority when operating within that scope. This theory of interrelationship was also central to the Supreme Court's famous decision related to President

Lincoln's authority to order disposition by prize courts of shipping captured during the initial stages of the American Civil War. In the *Prize Cases*, the Court endorsed this action by concluding that once war had been thrust upon the nation by states organized in rebellion, the President was authorized as commander in chief to exercise legal powers derived from the *jus belli.* Other seminal cases decided by the Supreme Court that involve exercises of wartime authority have echoed this theme. *Milligan*, *Quirin*, *Hamdi*, *Hamdan* are all examples of the Supreme Court relying on the law of war as a source of both authority and obligation implicitly invoked when the nation engages in armed hostilities.

There are of course other precedents that indicate that an irreconcilable conflict between domestic statute and international law should be resolved in favor of the statute. But there is nothing in the AUMF that even comes close to triggering this line of authority. Instead, the AUMF is far more analogous to the declaration of war that implicated the principle of military necessity in the Quirin decision, a fact that was not lost on the Supreme Court when 60 years later it invoked that precedent to support the authority of the government to preventively detain Mr. Hamdi.

Why the DC circuit Court of Appeals would ignore this tradition and assert that it need not consider the limits on national authority derived from the law of war is anyone's guess. It is however unfortunate that the court avoided the opportunity to analyze the range of important issues implicated by Al Bihani's detention: the legitimacy of Al Bihani's detention, whether the disqualification of the Taliban for POW status automatically infected militia groups that have associated themselves with the Taliban, how the law of armed conflict impacts the question of when preventive detention of nonstate belligerents should be terminated, why activities that are routinely performed by civilian contractors on behalf of the United States fall under the category of belligerent conduct when performed by members of enemy opposition groups. All of these questions are central to the legitimate continued invocation of authority derived from the principle of military necessity in relation to the armed component of the struggle against transnational terrorism; a principal is inextricably intertwined with the notion of all necessary means as that term is used in a congressional authorization to engage in armed hostilities against this threat. Ignoring the principle of military necessity in the context of all necessary means is inappropriate, unjustified, and inconsistent with the jurisprudential tradition that dates back to the very inception of the Republic. ■

Review Of Alan M. Dershowitz, *Is There A Right To Remain Silent? Coercive Interrogation And The Fifth Amendment After 9/11* (Oxford Univ. Press (2008)

By Tung Yin

Earlier this year, Pakistani-American Faisal Shahzad was arrested on terrorism-related charges for allegedly leaving a car bomb in Times Square, New York. The public soon learned that the arresting FBI agents had initially questioned Shahzad for about an hour before reading him his *Miranda* rights. This approach managed to provoke outrage from both civil libertarians and neo-conservatives. The civil libertarians argued that the Justice Department was trampling on the Bill of Rights in its rush to interrogate Shahzad, while the neo-conservatives denounced the President for not declaring Shahzad an enemy combatant to be tossed into a military brig.

Shahzad's case provides an opportune moment to review Professor Alan Dershowitz's recent book, *Is There a Right to Remain Silent? Coercive Interrogation and the Fifth Amendment After 9/11*, which was published in 2008. A prolific and provocative author, Dershowitz's past writings on subjects have ranged from his role in the Klaus von Bulow and O.J. Simpson murder trials to "torture warrants" to the Israel-Palestine conflict, and usually aimed at a broader audience. *Is There a Right to Remain Silent?* retains Dershowitz's readable style but, being an Oxford University Press monograph, delves deeply into legal history and doctrine at a level that lawyers and law professors can appreciate.

Summary

As the title indicates, Dershowitz contends that, under current doctrine, the right to remain silent is largely illusory. The government can induce, cajole, compel, or extract a confession from any of us, and our recourse, if any, is simply to exclude it in the event we are tried in a criminal case. Dershowitz uses *Chavez v. Martinez* (2003) as the focal point for his analysis of the meaning of the self-incrimination clause of the Fifth Amendment. In *Chavez*, criminal suspect Martinez was interrogated by a police officer after the suspect was badly wounded in a shootout. At the hospital, where Martinez was in severe pain awaiting medical treatment for his injuries, a police officer proceeded to interrogate him. The officer not only failed to read the familiar *Miranda* warnings, but also ignored Martinez's repeated requests for medical treatment. Under existing doctrine, Martinez's statements would likely be considered "compelled" within the meaning of the Fifth Amendment. However, Martinez was never charged with a crime and hence never faced a criminal trial. Instead, he brought a civil rights action against the interrogating officer under 42 U.S.C. § 1983, claiming a violation of his right to be free from self-incrimination. Although all Justices agreed that Martinez had been "compelled" to speak, a majority held that no Fifth Amendment violation had taken place because his statements were never used against him.

This distinction has immense significance for counterterrorism operations because, as Dershowitz notes, they are more concerned with the prevention of future crimes than with the investigation and prosecution of past crimes. If the Fifth Amendment does not proscribe any method of interrogation so long as the fruits of that interrogation are never used in a criminal trial, then presumably the Constitution would not prevent counterterrorism officers from resorting to coercion or torture to extract information from terrorism suspects. (Dershowitz does consider the Due Process Clause as a possible limitation on government conduct, but argues that its substantive, as opposed to procedural, limitations are too ambiguous under current doctrine to be relied upon.)

The bulk of the book is devoted to exploring the persuasiveness (or lack thereof) of the majority's reasoning in *Chavez*. Dershowitz devotes

Continued on **page 14**

Is There A Right To Remain Silent?, from page 13

considerable space to critiquing originalist arguments (such as the *Chavez* majority's) in favor of interpreting the self-incrimination clause. Among other things, he notes that historically, criminal defendants were barred from testifying and hence it would be nonsensical to view the primary purpose of the self-incrimination clause as protecting them from being compelled to testify. Dershowitz contends that the historical intent of the Framers is too ambiguous to draw any definitive conclusions about whether the self-incrimination clause should be seen as only an exclusionary rule. He therefore turns to the policies underlying the privilege as the starting point for determining what the privilege should protect. Here, he notes the three different privileges that have emerged: the defendant's privilege (i.e., not to be compelled to testify in a criminal trial); the witness's privilege (i.e., to refuse to answer questions under oath that would tend to incriminate oneself); and the suspect's privilege (i.e., not to be compelled to confess under coercive conditions, such as in a police station).

Recognizing the need for actionable information in counterterrorism operations, Dershowitz concludes his book by suggesting essentially that *Chavez* went too far: "The privilege against self-incrimination should be construed to impose restrictions on at least *some* means of coercion, even if the resulting information is never used against a defendant at a criminal trial." (p. 176) At the same time, he does not urge an absolutist interpretation: "Americans do *not* have an absolute right to remain silent . . . . [just as the] government does not have the absolute power to use all manner of coercive interrogation, even for preventative purposes."

Critique

Although the title of the book implies primary focus on post-9/11 (and hence terrorism/national security-related) interrogation, this is perhaps a bit of an oversell. *Chavez* was decided after 9/11 and perhaps in its shadow, but it is neither a terrorism nor national security case. Because the interpretative arguments that Dershowitz uses do lead him to a policy prescription, however, they nevertheless have relevance to counterterrorism operations.

At the outset, it is worth noting that the government need not necessarily be put to an either/or (but not both) choice of counterterrorism versus criminal enforcement. Dershowitz assumes that coerced confessions, while apparently not a Fifth Amendment violation, are nevertheless inadmissible in a criminal trial – an assumption that is generally, but not always true, as the Shahzad interrogation suggests. There, the Justice Department predicated its un-*Mirandized* questioning under the "public safety" exception to *Miranda*. The justification for the public safety exception is that the exigency of some circumstances is so great that society cannot tolerate the possibility that *Miranda* warnings might dissuade suspects from answering. Because the public safety exception not only permits un-*Mirandized* questioning but also allows the results of such interrogation to be admitted against the defendant, it represents a "win/win" for the government. Nevertheless, the public safety exception is supposedly narrow in scope, relating to imminent threats to the public. As there was no such threat to public safety present in *Chavez*, the statements made in response to that interrogation would not have qualified under the exception. Depending on what was asked, however, some incriminating statements by Shahzad might; for example, ask if Shahzad were questioned about whether he had left other truck bombs, an affirmative response would incriminate him, but it would also be admissible.

Dershowitz's ultimate conclusion – that, even in the post-9/11 world, there should be limits on interrogation methods – seems reasonable from a policy perspective, but it is not entirely clear why the self-incrimination clause limits on methods of interrogation should be drawn where he draws them. If the purpose of the self-incrimination clause is to ensure that we are not forced to tell the government things that we want to keep secret because they incriminate us, then it really depends on what "forced" means. Presumably no criminal defendant actually wants to admit his or her wrongdoing (with the exception of the rare defendant who pleads guilty without any plea agreement); they do so because they are *induced*

by the government's offer of leniency, whether in the form of a reduced sentence or dismissed charges or other benefits. Indeed, much academic literature has criticized the practice of plea bargaining precisely because the government's inducement is believed to overwhelm the defendant's capacity to resist – in other words, some scholars believe that plea bargains can *compel* defendants to admit to committing crimes when they would otherwise say nothing.

If the Fifth Amendment is about protecting people from being compelled to speak against themselves, it's unclear why Dershowitz would read the self-incrimination clause as prohibiting some kinds of coercion while allowing other kinds. Presumably, by "some means of coercion," he means torture or torture "lite" (i.e., waterboarding and the like), as opposed to reduced sentences or dismissed charges. But one might criticize the inherent malleability of substantive due process, its "shock the conscience" standard seems more suited to distinguishing between unacceptable negative coercion and acceptable positive inducements. Dershowitz does consider substantive due process as a limitation on government interrogation conduct but rejects it on doctrinal grounds. So long as one is discussing how the Constitution should be interpreted, however, one should be just as free to argue that current doctrine regarding the reach of substantive due process is unduly restrictive as to argue for a broader reading of the self-incrimination clause.

Conclusion

The doctrinal answer to *Is There a Right to Remain Silent?* appears to be "no." Whether this is a normatively desirable outcome may depend on one's general feelings about the war against al Qaeda and the degree to which one believes that ticking time bomb scenarios are even vaguely plausible in real-life. Alan Dershowitz's monograph provides a very good framework for thinking about the role, if any, that the self-incrimination clause should play in policing the government's power to extract answers from unwilling suspects. ■

Author bio: Tung Yin is professor of law, Lewis & Clark Law School.

"Like all Holmes' reasoning, the thing seemed simplicity itself when it was once explained"

The Memoirs of Sherlock Holmes, The Stock Broker's Clerk

By General John D. Altenburg, Jr.

Homeland Security: Legal and Policy Issues is a timely, sophisticated and valuable work. Published by the Section of Administrative Law and Regulatory Practice of the American Bar Association, this handbook exceeds the goal stated by the Publications Committee of the Administrative Law Section Council that the handbook "would capture for practitioners and the public alike, a number of areas critical to Homeland Security Law". This focused yet comprehensive guide is more than merely a series of law review-like articles. This handbook provides valuable guidance, understandable to attorneys and laymen alike. Without exception, the array of experts addressing the specific issues in the handbook, like Holmes himself, bring simplicity to these intricate and detailed requirements.

Each Chapter is actually a single article addressing a unique aspect of Homeland Security practice. The Chapters are structured in familiar fashion, initially providing the foundation of the law and policy, then addressing the intricacies specific to the subject matter of the article, and finally suggesting tips for compliance or implementation of the various laws and policies. The structure alone postures this handbook as a necessary tool for a wide range of practitioners. Corporate counsel, federal, state and local policy makers and their general counsel will all benefit by having this handbook on their shelves for ready reference.

A few specifics are noteworthy. Chapter 1, *"Homeland Security: An Inside Look of the Last Seven Years and a Look Ahead,"* provides a concise yet comprehensive policy development primer of the Department of Homeland Security. Congressional staff members, as well as general practitioners, would do well to answer the author's questions as she urges a reexamination of the recommendation of the Hart-Rudman Commission (which recommended establishing a Homeland Security Department less than a year before the September 11 attacks):

The ABA National Security Law Report

http://www.abanet.org/natsecurity/

The National Security Law Report (N.S.L.R.) contains articles concerning the law relating to the security of our Nation and associated topics. The N.S.L.R. is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee, the ABA, or any governmental agency or private enterprise. To receive the N.S.L.R., contact Holly Stewart McMahon at 740 15th St., NW, Washington, DC 20005-1009; (202) 662-1035; or hmcmahon@staff.abanet.org.

…[h]ave we made homeland security a necessary priority in our overall national security strategy? Have we adequately prepared the American people for potential threats? Do we have effective partnerships with international, state, local and tribal governments? Have we effectively eliminated government overlap and duplication? **(See page 20.)**

The final advice in Chapter 1 is the basis of a workable policy for an agency, corporation, or individual practicing and advising in this broad area, "If an incident did occur, there must be a clear chain of command and oversight to avoid chaos."

The "clear chain of command and oversight" are essential because the breadth and complexity of regulatory requirements is vast and technological changes are rapid. As important, there must be unity of direction for compliance and risk management that embraces the specific corporate or agency culture. It is not trite to remember the words of Henry David Thoreau, " In the long run men only hit what they aim at." The government's past efforts have demonstrated that security is only as good as the effective integration, communication, and unity of purpose of the myriad communities involved in these tasks.

Similarly, *"Compliance is Not Enough: What It Really Takes to Maintain Responsible Information Security."* (Chapter 5) is a superb primer on the "risk management" function for any practitioner advising corporate clients. The article discusses compliance schemes to meet diverse regulatory obligations in the context of business effectiveness and information technology. The author urges an "integrated" approach for IT operations which includes, "security, disaster recovery, business continuity, resilience and IT operations." This chapter alone prompts a focused read of the entire book. It is precisely the art of providing business context to the government's regulatory requirements which demands decision-makers' (whether corporate CEOs and Chairpersons or state, local, or tribal leaders) knowledge, direction and control of regulatory requirements and the implementation of internal control systems to meet those requirements.

Highlighting these chapters is not to imply negative comment of other chapters. Quite the opposite, every chapter provides valuable information and practical adaptations to 21st Century issues facing government and business. *"State and Federal Emergency Powers," (*Chapter 2) is a valuable discussion concerning disaster assistance and its effect on business. It should be read in conjunction with *"Succession Planning and Business Continuity,"* (Chapter 8) which discusses corporate requirements and potential liability of a wide range of corporate structures. It includes a section concerning oversight by directors and officers, as well as a best practices discussion.

"The 'clear chain of command and oversight' are essential because the breadth and complexity of regulatory requirements is vast and technological changes are rapid."

The salient impression when perusing this handbook is the vastness of highly regulated areas which may apply to any corporation, regardless of its core mission or product. The book highlights the government's focused and increased enforcement efforts in various areas. Whether implementing the requirements for the Transportation Workers Identification Credential (TWIC) (Chapter 11) or understanding US Northern Command's role in federal, state, local and

Continued on **page 18**

The Stock Broker's Clerk, from page 17

tribal emergency action (Chapter 3), the complex nature of individual regulatory schemes is fertile ground for noncompliance, inadvertent or purposeful. Increased penalties, including practical losses such as loss of the ability to execute core missions, loom for those who do not heed this book's solid advice.

This book is a must read for decision makers and advisors who deal with the many and diverse areas integral to the nation's security.

Many first editions immediately generate the need for a subsequent edition. This handbook, though essential reading, may cause the reader to question the bewildering array of multiple, distinct regulatory requirements. What may be missing is additional discussion of risk management programs, or oversight compliance programs, for those regulated areas affecting the core mission. Such programs are, in my opinion, necessary in today's regulatory environment. The best oversight programs assist the attorney practitioner to advise corporate decision makers concerning the requirements and effects of regulatory schemes. This is especially true of issues affecting the respective businesses in the context of the corporate culture and unique business processes.

This excellent handbook's next edition will also be enhanced by adding a chapter devoted to explaining the regulatory morass inherent in contract execution complicated by access to classified data. So-called classified contracts have become a significant percentage of all government contracts, especially in procurements related to national and homeland security. Execution of these contracts adds a regulatory layer to all the subjects addressed in this handbook. Subsequent editions may want to recognize the need for unified risk management compliance structures with appropriate oversight because classified contracts include issues associated with every Chapter of the handbook. For example, the scope and focus of issues discussed in Chapter 13 *"CFIUS and Foreign Investment,"* (Chapter 13) are exponentially intensified when a foreign entity, corporate or otherwise, offers to purchase a Department of Defense contractor handling classified contracts. (CFIUS is Committee on Foreign Investment in the United States; it reviews transactions that will result in foreign control of U.S. corporations.) Indeed, there are both statutory and regulatory requirements, some which may require Secretary of Defense waivers in order to complete the transaction.

This book is a must read for decision makers and advisors who deal with the many and diverse areas integral to the nation's security. This book is a welcome starting point for the practitioner. It makes clear that this subject is expanding so rapidly that it demands a strategic approach to compliance. Corporate counsel especially (often designated as "senior compliance officials") must eliminate "stove pipe compliance" structures. I cherish my copy of this edition; I look forward to an expanded edition. ■

Congratulations to **Mark A. Frazzetto**, 2010 winner of the ABA Standing Committee on Law and National Security National Security Law Student Writing Competition. His paper on "Protecting Against Economic Espionage: Trade Secrets, Standards, and Criminal Liability" will appear in the next issue of The *National Security Law Report.*

Mark is a part time student (4L) at Loyola University of Chicago School of Law.

Congratulations to **Adrian Snead,** 2009 winner of the ABA Standing Committee on Law and National Security National Security Law Student Writing Competition. His paper on Redefining Fourth Amendment Rights in the Digital Age is reprinted here.

"Note from the Author: Since originally submitting this article for publication in early August 2009, several new developments have occurred relating to suspicionless border searches of digital devices. In late August 2009, the U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) issued internal directives outlining their policy with regard to these searches. Additionally, on September 7, 2010, a federal lawsuit was filed in the Eastern District of New York against CBP claiming that the CBP's policy violates the First and Fourth Amendments. Finally, two bills were introduced in the House of Representatives in 2009 to address suspicionless border searches. This update includes information on all three developments."

Redefining Fourth Amendment Rights in the Digital Age: Suspicionless Border Searches of Electronic Data Storage Devices

Executive Summary

The world today is in many ways alien to the world Abraham Lincoln knew when he saved the Union and her Constitution. Communications move at the speed of light and an average laptop hard drive can store the same amount of information as was contained by all the books in the Library of Congress at the close of the Civil War. Yet, the constitution still guarantees protection from unreasonable searches and seizures of citizens' papers and effects. Today, courts and policy makers must find ways of respecting the Fourth Amendment while recognizing the new realities of digital data. To date, courts and the executive branch have maintained that suspicionless border searches of electronic storage devices do not violate the Fourth Amendment. This paper first examines whether such plenary power is constitutional. Second, this paper argues that even if such power is constitutional, exercising that power is bad policy. Lastly, this paper advocates the introduction and passage of an international treaty protecting travelers from arbitrary searches.)

I. The Issue: Suspicionless Border Searches Of Electronic Data Storage Devices.

Imagine this: you are an investigative reporter returning home from a trip overseas. You land at Dulles airport happy to see your home country. Just after a Customs and Border Patrol (CBP) officer stamps your passport and welcomes you home, another officer asks you to open your luggage. Understanding this to be a routine and random screening, you comply. However, you soon learn that this search will be anything but routine. You are told to turn over your laptop and all other electronic data storage devices to CBP agents so that they may copy all of your files. You protest, claiming your constitutional right to privacy and safety from unreasonable searches and seizures. You are told by CBP agents that this search is legal, and warned that if you refuse to comply you will not be allowed to reenter your country. Under duress, you reluctantly agree. Two weeks later, your computer and other memory devices are returned to you without explanation. Think this could not happen in America?

Continued on **page 20**

Redefining Fourth Amendment Rights, from page 19

It already has. Bill Hogan, an investigative reporter, experienced almost the exact scenario when he returned to the United State in February 2008, after vacationing in Germany. Alex Kingsbury, *Seizing Laptops and Cameras Without Cause*, U.S. News & World Report, June 24, 2008, http://www.usnews.com/articles/news/national/2008/06/24/seizing-laptops-and-cameras-without-cause.html.

In a similarly disturbing situation, CBP agents detained a graduate student, Pascal Abidor, on May 1, 2010, at the Quebec-New York border. Complaint at 4, *Pascal Abidor v. Napolitano*, 2010 WL 3477769 (E.D.N.Y. Sept. 7, 2010) (No. CV 10-4059). Mr. Abidor is a dual American and French citizen, and was a Ph.D. student at McGill University in Montreal. He was traveling home from Montreal to New York City on an Amtrak train when he was stopped and questioned during a border crossing. *Id.*

CBP agents learned that Mr. Abidor had previously lived in Jordan and had traveled to Syria. *Id.* Agents escorted Mr. Abidor to the café car, seized and turned on his laptop, and ordered Mr. Abidor to enter his password. *Id.* Mr. Abidor complied. *Id.* The agents found pictures of Hamas and Hezbollah rallies on the laptop. *Id.* Mr. Abidor explained that he had downloaded the images off Google, and that they were part of his doctoral research on the modern history of Shiites in Lebanon. *Id.* Approximately five hours later, after being handcuffed, searched, and providing his computer password in writing to CBP agents, Mr. Abidor walked out of a detention facility without his laptop, digital camera, two cell phones, or his external hard drive. *Id.* at 4-5. Mr. Abidor's property was not returned until May 12, at which time Mr. Abidor claims that he found that his files had been searched and likely copied, and that his external hard drive had been physically opened. *Id.* at 5-6.

On September 7, 2010, Mr. Abidor, along with the National Association of Criminal Defense Lawyers, and the National Press Photographers Association, sued the Secretary of the Department of Homeland Security (DHS), the Assistant Secretary of Homeland Security for U.S. Immigration and Customs Enforcement (ICE), and the Commissioner of the CBP in the Eastern District of New York. *Id.* at 1. The plaintiffs aver that such suspicionless of electronic devices violate the First and Fourth Amendments, and are seeking declaratory and injuctive relief against the DHS, ICE, and CBP. *Id.* at 14-15.

What Mr. Hogan and Mr. Abidor faced upon their return to the United States was a suspicionless border search of their electronic devices. A suspicionless search of an electronic devise is the copying or scanning of the data stored in a computer, smart phone, digital camera, or other electronic device's hard drive – the files and information contained in the memory – and not a physical examination of the device itself. *Laptop Searches & Other Violations of Privacy Faced By Americans Returning From Overseas Travel* before the Subcomm. on the Constitution of the S. Comm. on the Judiciary, 110th Cong. 155 (2008) (testimony of Larry Cunningham, Assistant District Attorney, Bronx District Attorney's Office, Bronx County, New York). By definition, a border search can occur at any point of entry into the United States, including airports anywhere in the country. *Id.* at 95 (*citing Almeida-Sanchez v. United States*, 413 U.S. 266, 272-37 (1973)). Currently, the law gives CBP agents plenary authority to search and copy all of a traveler's data upon that person's entry into the United States. DHS claims that such searches are necessary to keep Americans safe because data searches allow DHS to catch importers of child pornography, to recover stolen proprietary software, and to foil future terrorist attacks. However, critics point out that suspicionless data searches pose a threat to businesses, attorneys, and the government by compromising sensitive and secret data. The policy also provides a bad precedent that totalitarian regimes may emulate, threatens to exacerbate racial profiling, invades privacy, and chills First Amendment rights. Finally, suspicionless searches are impractical and can be easily subverted.

There are at least three avenues available to policy makers and the Court should they wish to change DHS border search policies with regard to suspicionless searches. First, the President can order DHS to institute new policies that safeguard

citizens' rights by requiring reasonable suspicion before conducting electronic data searches. Congress can pass a law to protect citizens and other travelers by requiring a reasonable suspicion standard. Finally, the Supreme Court can act by striking down the border search exception for electronic data.

However, the threat faced by businesses, attorneys, and the government by foreign governments conducting reciprocal suspicionless searches of incoming electronic devices demands that the President and Congress act together. The President should propose, and Congress should enact an international treaty, securing international travelers' data from suspicionless searches.

II. The Law Today Allows For Suspicionless Searches of All Electronic Storage Devices at the Border.

American law today is clear: "[R]easonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *United States v. Arnold*, 523 F.3d 941, 946 (9th Cir. 2008). In accordance with the wide latitude the law affords customs and immigration agents who conduct these searches, CBP and ICE both issued directives in August 2009, relating to border searches of electronic devices. *See generally*, Border Searches of Electronic Devices Containing Information, CBP Directive No. 3340-049 (Aug. 20, 2009); Border Searches of Electronic Devices, ICE Directive No. 7-6.1 (Aug. 18, 2009). The ICE directive does not require suspicion of any form on the part of its agents before they "search, detain, seize, retain, and share electronic devices, or information contained" in a travel's digital device. ICE Directive No. 7-6.1 at 2. The directive clearly states that a traveler's consent is *not* required before ICE agents commence a search. *Id.* at 4. The only circumstance where reasonable suspicion is necessary on the part of ICE agents is when they require "subject matter assistance" from other federal agencies. *Id.* at 6. The CBP Directive provides substantially the same language as the ICE directive. CBP Directive No. 3340 -049 at 3-5.

Historically, suspicionless data searches are the progeny of the border search exception, first officially recognized in 1977. *Laptop Searches* at 91 (testimony of Larry Cunningham). Writing for the majority in a 5-4 decision, then Justice Rehnquist held that border searches are "reasonable by the virtue of the fact that they occur at the border" because of the "long-standing right of the sovereign to protect itself" from incoming persons and property. *United States v. Ramsey*, 431 U.S. 606, 616 (1977). The Supreme Court has recognized two distinct types of border searches that invoke different constitutional protections: "routine" border searches, which do not require any suspicion, and non-routine searches, which require at least reasonable suspicion on the part of a CBP officer. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985). While the Supreme Court has not elucidated precise definitions for routine and non-routine searches, it has noted that non-routine searches include invasive searches that strike at the dignity of an individual, such as x-rays, body cavity searches, and strip searches. *Id.* at 541 n.4. Routine searches include searches of cargo, luggage, car components, and other property. *Laptop Searches* at 156 (testimony of Nathan Sales, Assistant Professor of Law, George Mason University School of Law). This suggests a bright line rule between property, where routine searches are allowed, and invasive searches of the body impinging on the dignity of the individual, which require more scrutiny. *Id.* at 158.

In formulating the border search exception, the Supreme Court's reasoning has largely focused on a historical review of laws and cases. To support his affirmation of the border search exception, Justice Rehnquist in *Ramsey* reached back to the first Congress. *Ramsey*, 431 U.S. at 616 (*quoting* 1 stat. 29, § 24). Before proposing the Fourth Amendment, the first Congress passed the first customs law, which gave government officials the power to search "any ship or vessel, in which they shall have reason to suspect any goods, wares or merchandise subject to duty shall be concealed. . . ." *Id.* Justice Rehnquist contin-

Continued on **page 22**

Redefining Fourth Amendment Rights, from page 21

ued his historical analysis by citing two other seminal rulings, *Boyd v. United States* and *Carroll v. United States*. *Id.* In *Boyd*, the Supreme Court held that the warrantless seizure, which presupposed a warrantless search, of 35 plates of imported glass did not violate the Fourth Amendment because the seizure of stolen goods imported illegally was authorized by common law, historically authorized by English statutes, and authorized by the aforementioned first custom's act. *Boyd v. United States*, 116 U.S. 616, 623 (1886). *Carroll* dealt with the suspicionless searches of cars at border crossings during Prohibition. *See Carroll v. United States*, 267 U.S. 132, 153-54 (1925). Chief Justice Taft, writing for the majority in *Carroll*, concluded in that it was reasonable, and therefore constitutional, for border agents to search vehicles entering the country because of the needs of "national self protection." *Id.*

Based on Justice Rehnquist's historical review, there is an emerging consensus among the circuit courts that suspicionless border searches of electronic storage devices raise no Fourth Amendment concerns. *Laptop Searches* at 157 (testimony of Nathan Sales). The Ninth and Fourth circuits, and district courts in the First, Third, and Fifth circuits have held that suspicionless searches are acceptable. *Id.* (internal citations omitted). Courts in the Second and Fifth circuits have not ruled on the constitutionality of suspicionless searches, because reasonable suspicion existed in cases brought before those courts. *Id.* (internal citations omitted). It is clear that the Fourth Amendment at the border does not protect citizens' electronic devices and the personal data they may contain.

However, the current border search exception is based, at least partly, on incorrectly interpreted precedent. The majority in *Arnold* cited *Ramsey* to support its affirmation of suspicionless data searches. *Arnold*, 523 F.3d at 944. Justice Rehnquist relied on the "historical importance" of the fact that the first Congress passed the first custom's act before it proposed the Fourth Amendment. *Id.* The act grants customs officials "full power and authority" to enter and search "any ship or vessel, in which they should have reason to suspect any goods, wares, or merchandise subject to duty shall be concealed." *Id.* (*quoting* 1 stat. 29, § 24). Justice Rehnquist then cites *Boyd v. United States* and *Carroll v. United States* in support of his determination that suspicionless border searches are permissible.

The 1789 statue cited by Justice Rehnquist appears to contradict his conclusion. The statute applied to "any ship or vessel," not to any person or citizen. Customs officials were granted their plenary power to inspect cargo if they believed that the ship or vessel contained "goods, wares, or merchandise subject to [a] duty." The statute clearly applied to merchants, as opposed to private citizens, because the search was to ensure the collection of taxes on incoming goods. The reference to ships or vessels also appears to disqualify goods carried by persons entering by land from Canada, Spanish Florida, or French Louisiana. The 1789 statute still required customs officials to have "reason" to suspect before searching a vessel. Lastly, the customs law would not have had to conform to the Fourth Amendment at the time of its passage; however, it would have been required to do so after the ratification of the Bill of Rights.

While Justice Rehnquist relied on *Boyd* to support his assertion of plenary power at the border, the court in *Boyd* found that the "search for and seizure of stolen or forfeited goods . . . liable to duties" was a "totally different thing[] from a search for and the seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him." *Boyd*, 116 U.S. at 623. The Supreme Court held that compelling a person to produce their private books and papers, and then to convict him of a crime based on that evidence is "contrary to the principles of a free government" and is "abhorrent to the instincts of an American." *Id.* at 631-32. The Court held that the order requiring Boyd to produce an invoice for his goods to be unconstitutional. *Id.* at 638. *Carroll v. United States* supports the interpretation that the Fourth Amendment protects a person's private papers but not his commercial possessions. *Carroll*, 267 U.S. at 153.

Precedent demonstrates that the Supreme

Court has historically allowed suspicionless border searches of physical property to prohibit the importation of contraband goods. However, searches of laptops and other data storage devices present a new and difficult issue because electronic data falls somewhere in the ether between property and person. Advancements in electronic storage have revolutionized the way people live, work, and do business. An average laptop hard drive with a capacity of 80 gigabytes can hold several million pages of text. Laptops have not simply replaced filing cabinets, rolodexes, and photo albums; they can contain a person's entire chat logs going back years, all photos they have ever taken, all intellectual property they may have created, and all files they have ever downloaded, purposefully or not. Therefore, while some contraband material, such as child pornography, can exist on a hard drive, it is likely to coexist with other personal and intellectual data.

A thorough search of thousands or hundreds of thousands of documents, as are contained on a laptop hard drive, would have been unlikely in the 1970s when Justice Rehnquist elucidated the suspicionless border search doctrine. While precedent allows customs officials to legally search each document, reading only enough for identification purposes, *Heidy v. United States Customs Service*, 681 F. Supp. 1445, 1450 (C.D. Cal. 1988), such a cursory search of millions of pages of documents and thousands of pictures or movie files, would have been impracticable before the advent of data mining technology, which can search all this data relatively quickly. Because data searches are aimed at discovering precise information contained in private documents, the old jurisprudence does not conform to the new realities of the digital age. The law has simply not caught up to the realities of the digital frontier.

III. Policy Arguments For And Against Suspicionless Border Electronic Data Searches.

DHS claims that suspicionless data searches are necessary to keep Americans safe because data searches allow DHS to catch importers of child pornography, to recover stolen proprietary software, and to foil terrorist attacks. However, critics point out that suspicionless data searches pose a threat to businesses, attorneys, and the government by compromising sensitive and secret data. The policy also provides a poor precedent that totalitarian regimes may emulate, threatens to exacerbate racial profiling, invades privacy, and chills First Amendment rights. Finally, suspicionless searches are impractical and can be easily subverted.

A. The Costs to Businesses, Attorneys, and Personal Privacy Outweighs the Benefits of Suspicionless Data Searches at the Border.

The Department of Homeland Security argues that requiring reasonable suspicion before conducting a border data search will inhibit DHS's ability to keep the nation safe by stopping criminals and terrorists from entering the United States. *See generally Laptop Searches* at 52-9 (testimony of Jayson Ahern, Deputy Commissioner, U.S. Customs and Border Protection). However, DHS's assertion is counterfactual. To date, there has not been a single case where a suspicionless laptop search uncovered terrorist activity. Laptop searches have been almost exclusively targeted toward finding child pornography. Thus far, there have been at least eleven cases challenging suspicionless laptop searches. Almost all dealt with child pornography prosecutions, and in nearly all cases, officers had reasonable suspicion to search. *Id.* at 156 (testimony of Nathan Sales). In at least one instance, a laptop search led to the discovery of stolen proprietary software on a traveler's computer. *Id.* at 54 (testimony of Jayson Ahern).

Moreover, it is unclear if the benefits of suspicionless data searches outweigh the costs to businesses, attorneys, and personal privacy. Fear of having secret business files compromised has resulted in businesses adopting costly security measures to secure confidential information during business trips. Businesses have purchase du-

Continued on **page 24**

Redefining Fourth Amendment Rights, from page 23

plicate laptops scrubbed of sensitive information to give to associates traveling abroad. *Id.* at 127 (testimony of Susan Gurley, Association of Corporate Travel Executives). Other measures include purchasing costly encryption software, sending files to themselves on web-accessible email, and developing secure virtual private networks (VPNs) to access the information via the internet. *Id.*

Attorneys face the same security concerns when traveling abroad. The attorney-client privilege is essential to the fair administration of justice and is a cornerstone of the American legal system. However, suspicionless searches of electronic equipment constitute a tremendous risk to the attorney-client privilege. Attorneys may now carry scanned copies of all documents relating to a case when they travel if such documents exist on their laptop. They may have digital photos of evidence on their computer or smart phones. Documents on their laptop will often have information relating to litigation strategy.

The fact that suspicionless searches appear to be triggered by having one's name on the terrorist watch list increases the risk to attorneys. *See id.* at 56 (testimony of Jayson Ahern); *See also id.* at 65 (testimony of Shirin Sinnar, Staff Attorney, Asian Law Caucus). It is conceivable an attorney representing a suspected terrorist or suing the federal government may have their name accidentally or purposefully placed on the watch list. If they travel internationally to collect evidence or for other reasons, they risk having their case and client information compromised when returning through immigration. The threat to business and legal travelers has lead Arnold & Porter, a large American law firm, to recommend to its clients that they take precautions to safeguard data before traveling overseas. Arnold & Porter, Client Advisory: *Working on the Flight?* February 2008. http://www.arnoldporter.com/resources/documents/CA-WorkingOnTheFlight-021208.pdf.

B. Suspicionless Data Searches Set a Poor International Precedent Likely to be Copied by Corrupt Regimes.

Other critics point out that border laptop searches create a bad precedent that totalitarian regimes can copy to steal trade or political secrets. *Laptop Searches* at 163 (testimony of Peter Swire, Professor of Law, Moritz College of Law, The Ohio State University). Regimes in China, Vietnam, Russia, and other developing nations in Africa may institute a policy of singling out business travelers or those with suspected ties to the American military and regularly copy all their electronic data in the name of "border protection." Given the fact that a 2008 Government Accountability Office report found that 70% of sensitive governmental data is not encrypted on government laptops and other mobile devices, foreign data searches of American government officials pose a particular threat to sensitive government files. Grant Gross, *Most Sensitive Data on Government Laptops Unencrypted*, July 29, 2008, PC World http://www.pcworld.com/businesscenter/article/149080/most_sensitive_data_on_government_laptops_unencrypted.html. This could lead to the leaking of trade, political, or military secrets. The United States would be in a poor position to complain, as those nations will no doubt cite American policy in defense of their own policy. A greater threat is the possibility that nations in Africa with suspect records of data protection and a reputation for corruption may steal travelers' personal financial information. Laptops and cell phones can contain sensitive credit card and bank account information, which can be used to perpetrate identity theft and financial fraud.

C. Suspicionless Data Searches Threaten to Exacerbate Racial Profiling and Are a General Invasion of Privacy.

Beyond breaching the reasonable person's expectation of privacy, evidence suggests that

Customs Border Patrol agents target racial and religious minorities for suspicionless data searches. There appear to be no CBP regulations prohibiting searches based on answers travelers give to questions regarding their religious and ethnic affiliations. *Id.* at 66 (testimony of Shirin Sinnar). In fact, some travelers have been asked questions about their religious beliefs. *Id.* at 62; *Id.* at 149 (statement of Asian Law Caucus, et al.).

Because laptops, cell phones, and personal digital assistants contain vast amounts of personal data, they are a repository of personal information akin to a personal filing cabinet in a home. Traditionally, people kept their most personal documents in the home filing cabinet. Bank records, credit card receipts, passwords, wills, phone records, and tax returns were all stored in the home safe from prying eyes and government agents. Today, banks and phone companies offer incentives to have customers download statements instead of having a hard copies mailed to their home. Wills can be scanned for safekeeping, passwords may be stored in a word document, and other files may contain thousands of pages of chat logs, emails, and other personal communications. While the filing cabinet may have kept some very personal communications, it is doubtful that a person would have been able to keep the range and breadth of personal letters that is apparent within email files alone. The very nature of personal computing today makes a personal filing cabinet in a home almost obsolete. However, unless someone was moving to the United States, it would have been highly unlikely that they would have transported all these personal documents with them every time they traveled. Therefore, it should be axiomic that people have the same expectation of privacy when it comes to data stored on their hard drive or other data storage device as with a personal filing cabinet within a home.

D. Suspicionless Border Searches Chill First Amendment Rights.

Invasive data searches chill First Amendment rights when travelers who fear the invasion of their privacy decline to store politically critical documents on their portable electronic devices. While limited readings of written material is necessary to identify the object, reading documents for the "purpose of revealing the *intellectual content* of the writing requires encroachment upon first amendment protections far beyond the mere search and seizure of materials." *Heidy*, 681 F. Supp. at 1450. What's more, retaining copies of material found not in violation of American law is "particularly obnoxious under the first amendment" and can "impermissibly 'chill'" a person's conduct of protected expression. *Id.* at 1452.

E. Suspicionless Data Searches Disproportionally Harm Innocent Travelers While Semi-Sophisticated Criminals Can Subvert the Searches.

Semi-sophisticated terrorists and other criminals can circumvent data searches by emailing themselves files over secure and encrypted networks, or by buying sophisticated encryption software that can hide certain files when a non-authorized person attempts to view an otherwise encrypted file. *Laptop Searches* at 172 (testimony of Peter Swire). Travelers making routine commutes for vacation or business have no incentive to buy expensive hardware or software, or to send thousands of files to themselves to ensure their privacy. Therefore, it is likely that intrusive laptop searches will affect innocent Americans and international travelers who do not intend to commit a crime, while criminals and terrorists find ways of subverting the system.

F. Suspicionless Data Searches Ask That Americans "Trust The Government" With Their Personal Data.

"Trust us, were from the government and we're here to keep you safe." This is the message CBP is essentially sending the American and international public regarding border searches. As

Continued on **page 26**

Redefining Fourth Amendment Rights, from page 25

it stands today, there is no congressional oversight of the border search program. The CBP would like the public to trust that it will not misuse its power to copy electronically stored material. However, repeatedly, intelligence agencies have misuse their authority. In October 2008, ABC News revealed that the National Security Agency used warrantless wiretaps to listen to Americans' overseas phone conversations, including private phone sex. Brian Ross, Et al, *U.S. Officers' "Phone Sex" Intercepted; Senate Demanding Answers*, October 9, 2008, ABC NEWS http://abcnews.go.com/print?id=5987804. Fear that government would misuse its powers, or the assumption that government would misuse its power, helped end a Clinton Administration initiative to place a "Clipper Chip" in electronic devices. *Laptop Searches* at 165 (testimony of Peter Swire). The chip would have allowed the federal government access to all encryption information. *Id.* Continuing to allow suspicionless data searches is likely to lead to misuse and abuse.

IV. Policy Makers Should Act to Prohibit Suspicionless Border Searches of Electronic Data.

It is clear that the costs to business and personal privacy outweigh the benefits of suspicionless border searches. The executive or Congress could act independently to require reasonable suspicion before CPB conducts data searches. For example, DHS could issue new guidelines requiring detailed record keeping of data searches, and make those records available for public and congressional revive. DHS could also issue new policy guidelines prohibiting its agents from conducting laptop searches without reasonable suspicion. Intelligence agencies could also work in unison and develop human capital to assess possible threats, and search only individuals that pose an imminent danger to the United Sates, while screening out the everyday traveler.

Congress has attempted to strengthen traveler's privacy protections. Senator Russ Feingold introduced S. 3612 during the 110th Congress. The act would have prohibited searches of American residents' electronic equipment without reasonable suspicion that the person was carrying contraband or was otherwise not entitled to enter the country. The bill would have disallowed seizures of equipment without a warrant or an order from the Foreign Intelligence Surveillance Court. The bill set procedures for searches including requiring records of the nature and reasons for searches, the presence of at minimum two DHS employees during searches – one of which was to be a supervisor – and that the search take place in a secure environment. The bill would have also prohibited profiling, set specific procedures and timelines for obtaining a search warrant before seizing equipment, limited access and disclosure of seized data, and established guidelines for the compensation and loss of data. The bill, introduced to the Committee on Homeland Security and Governmental affairs on September 26, 2008, was never voted out of committee. Two similar bills introduced during the 111th Congress, H.R. 239 and H.R. 1726, have likewise languished in committees.

The realities of the digital age and the current international travel environment demand greater protection of traveler's data. Businesspersons, attorneys, members of the armed services, members of Congress, congressional staffers, executive agency staff, and private citizens traveling internationally or simply transiting a United States airport should not be subject to invasive data searches simply because they carry electronic equipment. The threat of other nations conducting reciprocal data searches to steal business or military secrets from Americans traveling overseas should spur Congress and the President to act jointly. The president should propose, and congress should ratify an international treaty protecting personal data. Ideally, such a treaty would not only ban suspicionless data searches of incoming travelers, but all data searches at the border. Only with such an international instrument could travels feel that their privacy is secure when traveling internationally. ■