Civilian Research Project

The War on Terror, Intelligence Convergence, and Privacy

By

Lieutenant Colonel Steven P. Haight
United States Army

United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Senior Service College Fellowship. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
31-05-2012	Civilian Research Paper	

4. TITLE AND SUBTITLE

The War on Terror, Intelligence Convergence, and Privacy

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LTC Steven P. Haight, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Office of the Director of National Intelligence
Office of General Counsel
Liberty Crossing II
Washington, DC 20511

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Ave.
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A: UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Historically, the practice of the U.S. government was to maintain virtual and legal walls between law enforcement, the intelligence community, and the military. After the attacks on 9/11, it became readily apparent that the goal of comprehensive national security would require an unprecedented melding of those three communities and a drastic increase in intelligence integration as well as information sharing. Accordingly, various laws, executive orders, programs, and policies were implemented to facilitate this culture change. The lines of demarcation between the traditional roles of policeman, spy, and soldier have become increasingly blurred. While obviously the goal is for greater collective national security, does the current legal framework constructed to that end meet its intent while still preserving individuals' civil liberties and privacy? This paper considers the necessary yet delicate balance between information sharing and privacy protection.

15. SUBJECT TERMS

Military, Law Enforcement, Civil Liberties, Commissions, FISA, Information Sharing

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED	34	

USAWC CIVILIAN RESEARCH PROJECT

THE WAR ON TERROR, INTELLIGENCE CONVERGENCE, AND PRIVACY

by

Lieutenant Colonel Steven P. Haight
United States Army

Susan Gibson,
Deputy General Counsel, ODNI
Project Adviser

This CRP is submitted in partial fulfillment of the requirements of the Senior Service College fellowship.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Steven P. Haight

TITLE: The War on Terror, Intelligence Convergence, and Privacy

FORMAT: Civilian Research Project

DATE: 31 May 2012 WORD COUNT: 8,691 PAGES: 34

KEY TERMS: Military, Law Enforcement, Civil Liberties, Commissions, FISA, Information Sharing

CLASSIFICATION: Unclassified

Historically, the practice of the U.S. government was to maintain virtual and legal walls between law enforcement, the intelligence community, and the military. After the attacks on 9/11, it became readily apparent that the goal of comprehensive national security would require an unprecedented melding of those three communities and a drastic increase in intelligence integration as well as information sharing. Accordingly, various laws, executive orders, programs, and policies were implemented to facilitate this culture change. The lines of demarcation between the traditional roles of policeman, spy, and soldier have become increasingly blurred. While obviously the goal is for greater collective national security, does the current legal framework constructed to that end meet its intent while still preserving individuals' civil liberties and privacy? This paper considers the necessary yet delicate balance between information sharing and privacy protection.

THE WAR ON TERROR, INTELLIGENCE CONVERGENCE, AND PRIVACY

It is generally accepted the Cold War lasted from 1945 to 1991. This conflict pitted the potential military might of the United States and its NATO allies against the Soviet Union and the Warsaw Pact. Concurrently, as these two superpowers prepared for potential war, their intelligence arms, the CIA and KGB, struggled against each other in the arenas of espionage and counterintelligence. Meanwhile, on the domestic front, within this timeframe, the concepts of limited police power, the proper role of law enforcement, and reasonable expectation of privacy were being formulated and articulated by the Warren Court. The basic components of national security; namely, intelligence, military, and law enforcement; were largely compartmentalized and virtual walls of division were erected by policy, statute, and practice.

This practice of virtual and legal walls between the three communities seemed logical as their methods, missions, and typical adversaries were distinct. While the intelligence community and the military shared an overseas focus on threats posed by nation-states, one was spy vs. spy while the other was massing unit formations against their uniformed counterparts. Here in the States, local and federal law enforcement generally concentrated on reactive investigations of already occurred crimes and the hopeful arrest and successful prosecution of those crimes' perpetrators. After the attacks of September 11, 2001, it became readily apparent that the goal of comprehensive national security would require an unprecedented melding of those three communities and a drastic increase in intelligence integration as well as information sharing. Accordingly, various laws, executive orders, programs, and policies were implemented to facilitate this culture change. The lines of demarcation

between the traditional roles of policeman, spy, and soldier have become increasingly blurred. While nobody would argue the value of greater national security, some question the appropriate cost, if any, to individuals' civil liberties and privacy.

Walls, Walls, and More Walls:

None of these several walls of separation were monolithic or without significant holes. However, they did represent the then-existing desire to keep the authorities of law enforcement, intelligence, and the military distinct and separate. First, police work and soldiering have long been viewed as fundamentally different. For example, the Posse Comitatus Act[1] is a clear and specific prohibition on the use of the military for law enforcement purposes. Along with the posse comitatus prohibition, in existence since 1878, federal law restricts the direct participation of military personnel in law enforcement by compelling the Secretary of Defense to

> prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.[2]

An even more obvious manifestation of the wall between law enforcement and the military was the concrete notion that any meting out of criminal process or justice by the military was to be confined to those within their own ranks and subject to the Uniform Code of Military Justice. A basic tenet of military justice is that the jurisdiction of a court-martial is narrowly prescribed.[3] While the history of military tribunals outside of courts-martial and their application to citizens and foreign nationals is long and somewhat convoluted, the Supreme Court made it very clear in *Ex parte Milligan*[4] that the overlap between the military and law enforcement was nothing if not extremely

problematic. Upon discussing the differing concepts of law utilized to govern the nation's uniformed forces, martial law, and military government; the Court ruled that military courts could not try civilians when the civilian courts were still in operation.[5] The need for distinct spheres of military and civilian law enforcement was explained in the strongest of terms:

> If this position is sound to the extent claimed, then when war exists, foreign or domestic, and the country is subdivided into military departments for mere convenience, the commander of one of them can, if he chooses, within his limits, on the plea of necessity, with the approval of the Executive, substitute military force for and to the exclusion of the laws, and punish all persons, as he thinks right and proper, without fixed or certain rules.
>
> The statement of this proposition shows its importance, for, if true, republican government is a failure, and there is an end of liberty regulated by law. Martial law, established on such a basis, destroys every guarantee of the Constitution, and effectually renders the military independent of and superior to the civil power…. Civil liberty and this kind of martial law cannot endure together; the antagonism is irreconcilable; and, in the conflict, one or the other must perish.[6]

Consequently, any mixture of the roles of criminal investigator, prosecutor, and soldier required nuance and a soft touch.

Second, while the military is and always has been an enormous collector as well as consumer of intelligence, there are important divisions between military intelligence activities and civilian national intelligence operations. There is a fundamental difference between soldier and spy. Soldiers wage war, and if they do so in accordance with international law and custom, they are afforded certain protections such as prisoner of war status and combatant immunity. Spies, on the other hand, are afforded no such protection.[7] While that is an internationally accepted distinction between the military and intelligence operative, the domestic wall is founded in their different authorizing statutes. How the military, the Department of Defense, and the individual services are

organized and what roles they play are largely governed by Title 10 of the United States Code.[8] However, somewhat counterintuitively, much of the authority for the intelligence community is found in title 50, named War and National Defense.[9] Delineating between the military and intelligence communities is described by Andru Wall as a "long-simmering debate within the national security community over Title 10 and Title 50 authorities."[10]

> The Title 10-Title 50 debate is the epitome of an ill-defined policy debate with imprecise terms and mystifying pronouncements. This is a debate, much in vogue among national security experts and military lawyers over the past twenty years, where one person gravely states "there are some real Title 10-Title 50 issues here," others in the room nod affirmatively, and with furrowed brows all express agreement. Yet the terms of the debate are typically left undefined and mean different things to different people.[11]

The accepted state of confusion aside, the debate is evidence of a long-standing desire to separate the roles, missions, authorities, oversight, and "rice bowls" of the military from those of intelligence agencies.

One virtual brick, albeit a large one, in the perceived military-intelligence wall is that of covert action. The authority to conduct covert action, typically within the purview of the Central Intelligence Agency, and the requirement of a presidential finding are codified in the National Security Act as well as Executive Order 12333.[12] Under both provisions, the definition of covert action specifically excludes traditional military activities. Understandably, this distinction sets up a war of words and interpretation when trying to distinguish between "active" intelligence operations such as covert action and the military's "passive" intelligence operations described as mere operational preparation of the battlefield.[13]

Third, probably the most discussed and analyzed division between the components of national security was the wall between intelligence and law enforcement. Signed into law by President Truman, the National Security Act of 1947 created the Central Intelligence Agency. Significantly, Congress mandated the CIA to "have no police, subpoena, or law enforcement powers or internal security functions."[14] Later, Congress specifically stated, "The intention of the law was to hold intelligence separate and distinct from law enforcement activities. At the time the Act was written, there was concern about creating a monolithic central security service that history - and observations made of totalitarian states – had taught us was undesirable in a democratic society."[15] While it was recognized that the intelligence community and law enforcement had overlapping interests, there was a distinct separation between their authorities, methods, goals, and cultures.

This chasm only widened in the early 1970's. In the 1972 *Keith* case[16], the Supreme Court held "the Fourth Amendment prohibited warrantless surveillance directed at domestic threats to U.S. national security."[17] Then, in reaction to Watergate and other "scandals that involved overreaching into U.S. domestic areas by the Intelligence Community and improper domestic intelligence activities by the Law Enforcement Community,"[18] several investigations were conducted. The Rockefeller Commission, the Senate's Church Committee and the House's Pike Committee all revealed illegal activity by both the CIA and the FBI. "One of the unwritten but significant side effects of these investigations was behavioral in nature. The years that followed the investigations were marked by some reluctance on the part of the two cultures to form interactive relationships."[19] This reluctance only increased with the

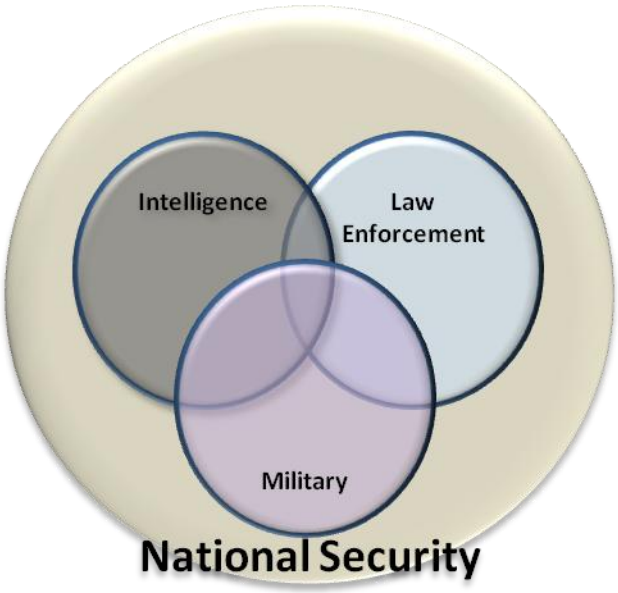
judicial interpretation of the new foreign intelligence tool, the Foreign Intelligence Surveillance Act (FISA).[20]

In the previously discussed *Keith* case, the Supreme Court expressly reserved the question of ability to conduct warrantless electronic surveillance when it comes to foreign powers. In response, President Carter signed FISA into law in 1978. It established "that non-criminal electronic surveillances within the United States were only permissible for the purpose of collecting foreign intelligence and/or foreign counterintelligence."[21] Whereas the probable cause standard required by the Warrant Clause of the Fourth Amendment entails a belief of criminality, the probable cause standard required by FISA entails only a belief that the target is a foreign power or an agent of a foreign power.[22] From its earliest application, FISA wire taps and searches often revealed evidence of crimes. When the use of FISA-obtained information in criminal prosecutions was challenged, the courts allowed it to the extent "the purpose thereof had been to secure foreign intelligence information rather than being primarily oriented towards assisting a criminal investigation or prosecution…. [T]hese cases served as the genesis of the so-called 'primary purpose' test and as the catalyst for the view that foreign intelligence investigations and criminal investigations had to be kept separate from each other."[23] This "primary purpose" requirement became practice and then written policy and ultimately came to be generally referred to as "the wall."

> An inescapable consequence of "the wall" was the inhibition of the sharing of information between the intelligence and law enforcement communities. In the 1990's and into the early 2000's, the two communities attempted to resolve their differences and concerns over this policy with the express purpose of improving information sharing between the two communities. While serving to highlight the difficulties of changing long-ingrained cultures, those efforts were largely unsuccessful, however.[24]

The Walls Come Tumbling Down:

On September 11, 2001, the United States was attacked by an international terrorist organization engaged in criminal activities. The relationships between the military, law enforcement, and the intelligence community would never be the same. The 9/11 Commission Report labeled our country and its components of national security as unprepared.[25] In order to prevent future attacks and address new forms of threat, the walls had to come down or, at a minimum, be re-looked and modified. The main impetus behind this convergence was the compound nature of the enemy; specifically, a terrorist being part criminal, part combatant, part spy. Accordingly, each of the walls was affected, and the three components now work together in vastly new and integrated ways, means, and methods. The bleed-over is not clean and the lines are not clear-cut. However, the three components now coalesce with the most obvious example of the point of fusion being the war on terror.



Change is typically uncomfortable, especially within bureaucracies, governments, and cultures. It is far beyond the reach of any single paper to analyze the myriad ways that these communities now increasingly intermingle. However, some of the more prevalent examples of de-compartmentalization and their accompanying criticism and growing pains will be presented.

First, the military and law enforcement are now coupled to an unprecedented degree. The simplest explanation of this result, again, is that a terrorist is an amalgamation of a criminal and combatant. A mere three days after the 9/11 attacks, Congress passed the Authorization for Use of Military Force.[26] This joint resolution's explicit language and reference to the War Powers Resolution made it abundantly clear that the U.S. was in a state of war against terror, an activity better described up to that point in time as a crime. This declaration created the following condition:

> Federal officials face the unprecedented situation of having to respond immediately to crisis events that are both war and crimes. This new paradigm of warfare has blurred the previously more-or-less clear line between national defense and law enforcement. And the idea of national defense is changing to encompass a broader range of threats than historically posed by a warring nation-state.
>
> Historically, "war" has been only between states…. Except for civil wars, acts of individuals and groups not qualifying as states have been deemed crimes either against the law of a particular state or violators of the "law of nations," e.g. piracy…. This country's initial legal response to terrorism in the 1980s was a law enforcement approach which extended the jurisdiction of the United States to criminal acts against Americans abroad.
>
> The realization, however, that non-state and clandestinely state sponsored groups now have the ability and willingness to employ means of mass destruction has dictated the recognition that states no longer have a monopoly on war. Therefore, it has become appropriate to use war powers against foreign terrorist organizations. Using those war powers against foreign terrorists operating within the United States calls for an understanding of when actions of force or terrorism by non-state groups should be treated pursuant to national security powers, rather than within the domain of law enforcement.[27]

This notion that the homeland now faced a hybrid criminal/enemy belligerent threat led to new missions for the nation's armed forces. For example, established October 1, 2002, the U.S. Northern Command's stated mission is to "partner to conduct Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests."[28] While this sounds well and good, some civil liberties advocates fear military overreaching and the militarization of the homeland, pointing out that the NorthCom Commander is the first "general since the Civil War with operational authority exclusively over military forces within the U.S."[29]

Treating combatants also as criminals poses an interesting question: What is the end state? Prisoners of war are not detained awaiting trial; they are detained pending cessation of hostilities. However, in the global war on terror, when exactly would that occur? Accordingly, soldiers are acutely aware that enemy combatants may eventually be tried in a court of law. With a criminal trial on the horizon, the role of soldier is transformed into one of law enforcement. Soldiers who were trained in combat operations, actions on the objective, capturing the enemy, and gathering military intelligence are now called upon to perform the functional equivalents of arresting a suspect, processing a crime scene, and collecting evidence. "Troops trained to kick down doors and shoot the enemy spend just as much time bagging and tagging evidence, photographing raid scenes and grilling suspects. That means American soldiers often assume the job of police investigators, even in the midst of an assault."[30]

Turning to that trial on the horizon, the use of military commissions is probably the best example of the fusion between the military and law enforcement in order to

combat terror. In response to questions by the Senate Judiciary Committee, Attorney General Holder declared:

> The United States is committed to using all lawful and appropriate authorities to win the war against al Qaeda and associated forces, including military, intelligence, law enforcement, diplomatic, and economic powers. When a suspected terrorist is apprehended abroad, whether military or law enforcement authorities will be used to detain him and address the threat he poses depends on all the facts and circumstances of the case, the context in which the apprehension occurs, and what is in the best interest of our national security. Since September 11, the U.S. government has used both military and law enforcement authorities to detain terrorists apprehended abroad, depending on the circumstances. Likewise, the decision whether to employ a civilian court or a military commission to prosecute a terrorist apprehended abroad is based on all the facts and circumstances of the case and what is in the best interest of national security. Where appropriate and in our national security interests, we will make every effort to prosecute suspected terrorists apprehended abroad – whether in civilian court or military commission.[31]

The debate about wither terrorists should be tried exclusively by military tribunal, only by Article III courts, or by either depending on the circumstances is indeed heated.

The history of the current military commissions is one of fits and starts. As discussed earlier, *Ex Parte Milligan* stood for the proposition that military tribunals lacked jurisdiction over civilians, at least under certain circumstances. Then, in a 1942 case involving German saboteurs captured by the FBI on U.S. soil but placed in military custody and tried by military commission, the Supreme Court ruled that military commissions did have jurisdiction over unlawful belligerents, to include over one who claimed U.S. citizenship.[32] Regardless, military commissions experienced various iterations and faced denouncement, formal disbandment, and multiple legal challenges and adverse rulings, most notably the *Hamdi*,[33] *Hamdan*,[34] and *Boumediene*[35] cases. For better or worse, military commissions currently operate under the authority of the Military Commissions Act of 2009.[36] In an extremely comprehensive comparison

between federal courts, military commissions, and law of war detention along with a thorough analysis of the advantages and disadvantages of each, former Assistant Attorney General for National Security, David Kris, persuasively argues that none of these courses of action should be abandoned, "we should continue to use all of the military, law enforcement, intelligence, diplomatic, and economic tools at our disposal, selecting in each case the particular tool that is most effective under the circumstances, consistent with our laws and values."[37]

Second, the military and intelligence community in this country have also merged to a degree unseen since the formation of the CIA. The visible and most public tip of this convergence iceberg is a simple matter of who is doing what. The current CIA Director is retired General David Petraeus, coming out of his three most recent military assignments as Commander of International Security Assistance Force and U.S. Forces Afghanistan, U.S. Central Command, and Multi-National Force Iraq. His predecessor at the CIA, Leon Panetta, is now the Secretary of Defense, taking over for Robert Gates, also a former CIA Director. Also, the current Director of National Intelligence is retired Air Force Lieutenant General James Clapper, Jr. Perhaps the most intriguing by-name example of convergence is General Keith Alexander who is dual-hatted as the Director, National Security Agency and Commander, U.S. Cyber Command and routinely expected to shift between his title 10 and title 50 responsibilities. The "blurring of lines between soldiers and spies" and the inevitable result that "military and intelligence operatives are at times virtually indistinguishable from each other" is fairly evident.[38] Critics, from inside both communities, argue this blurring distorts the CIA's "historic

mission as a civilian espionage agency and [has] turned it into an arm of the Defense Department."[39]

The Osama bin Laden raid, the Al Awlaki strike, and the drone program are all examples of military-intelligence convergence. Another obvious, and also very public, example of the melding of the soldier's and spy's cultures is Executive Order 13491 which now prohibits the CIA from using any interrogation methods not found in the U.S. Army Field Manual.[40] Unquestionably, American intelligence has become more militarized as "intelligence services always become more militarized during war, and the United States has been at war for [over] ten years."[41] This militarization of intelligence is not met without a certain amount of skepticism. The critiques take different forms but can be sorted into one of three basic complaints about oversight, focus and competency, or budget and resources.

"The real problem with the militarization of American intelligence is that it obscures and loosens lines of authority and responsibility."[42] When these lines are obscured, blind spots in congressional oversight are created because of the glaringly obvious fact that intelligence committees are briefed on intelligence operations whereas the military reports to armed services panels.[43] Turning to training and expertise, some fear that to the extent that the intelligence community becomes more of just a para-military actor, the "most important mission of intelligence gathering, analysis, and reporting can become endangered. Maybe in theory an organization can do very different things well, but in the real world, it's hard; leaders naturally become focused on one big mission or the other. The para- military function/mission is very different from the intelligence one."[44] Some view that the inclination to delve into what are historically

other's roles is at its core a competition over personnel, resources, and budgets in an era of increased austerity. Regardless of the tack, many want all concerned to just stay in their perceived lanes. As one stated, "Call me old fashioned, but I prefer the method of one hat to one person, where warriors fight wars, rather than gather intelligence; intelligence officers gather intelligence, rather than fight wars; and contractors work in the workplace, rather than the battle space."[45]

The observation and analysis of military-intelligence convergence is commonly known as the Title 10/Title 50 debate. The discussion is so labeled due to the shorthand distinctions between intelligence and military operations. Some have argued, with little traction, to create a "Title 60" that simply erases the distinctive lines of authority altogether. Professor Robert Chesney offers a more measured approach. He recognizes that convergence has disrupted the ill-suited domestic legal architecture or framework, specifically "on key elements in that framework, especially those that rely on categorical distinctions that convergence confounds (like the notion of crisp delineations among collection, covert action, and military activity)."[46] Furthermore,

> The key issues include the increasingly large and significant set of military operations that are subject neither to presidential authorization nor legislative notification; lingering suspicion with respect to whether and why the CIA might be at greater liberty than JSOC[Joint Special Operations Command] to conduct operations without host-state consent; and the difficulty of mapping the existing architecture onto operations in cyberspace.[47]

After pointing out the difficulties in accountability that convergence has created, Professor Chesney does offer normative recommendations that are far more realistic than a call for everybody to simply mind their own rice bowls.

Clearly, the most obvious erosion of role distinctions motivated by the war on terror is to the wall between the intelligence community and law enforcement. As

discussed above, due to judicial interpretation and certain policies, there was a belief "that no FISA information could be shared with agents working on criminal investigations."[48] "This perception evolved into the still more exaggerated belief that the FBI could not share any intelligence information with criminal investigators, even if no FISA procedures had been used. Thus, relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators."[49] This dynamic would not be tolerated after 9/11. It has been described, "The attacks of September 11, 2001, destroyed the World Trade Center and a portion of the Pentagon; they also demolished the wall between U.S. law enforcement and intelligence."[50] After the attacks, it was immediately expected that counterterrorism would now not only involve all parts of the U.S. government but also be based upon extensive information sharing between those elements.

To that end, the USA PATRIOT ACT became law 26 October 2001.[51] One of its multiple effects was to bring down the wall and enhance information sharing, back and forth, between the two communities. It accomplished this by changing "the requirement that 'the purpose' of a FISA surveillance be to collect foreign intelligence information to require that collecting such information be 'a significant purpose' of FISA electronic surveillance or physical search."[52] After a significant legal challenge, the Foreign Intelligence Surveillance Court of Review upheld this change in its opinion on November 18, 2002.[53] "Thus, 'the wall' tumbled into a grave well dug for it by the Court of Review."[54]

Many other organizational changes occurred which, in helping to bring down walls and stovepipes, transformed the U.S. government from a "need to know" culture

into one of a “need to share” way of thinking. In 2002, the Department of Homeland Security was created, reconfiguring the government and combining 22 agencies into a new Cabinet agency.[55] Then, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) established the Office of the Director of National Intelligence as well as the National Counterterrorism Center.[56] These federal organizations were charged to ensure maximum information sharing. Specifically, IRTPA also established the Information Sharing Environment, charged with government-wide jurisdiction to facilitate availability of and access to information.[57] The changes were not limited to the intelligence community as the law enforcement side was also revamped. While a call for a new domestic agency was rejected, the FBI shifted its long favored focus on criminal justice over to its national security mission, and the Department of Justice shifted resources from its Criminal Section to a newly formed National Security Division. This drive fully integrated the FBI into the overall intelligence effort.

This massive reorganization not only aims to enhance integration and information sharing at the national level, but down to the state and local levels as well. All must chip in as threats take on the various forms of terrorism, illicit financing, drug smuggling, and other transnational crimes. Fully integrated Regional Joint Terrorism Task Forces were formed. Yet another example is the development of state and local fusion centers. “The fusion center has ‘emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence.’”[58] These centers combat both crime and terrorism by “harvesting and analyzing data from law enforcement, public safety, and private sector sources.”[59] Their efforts bring state and

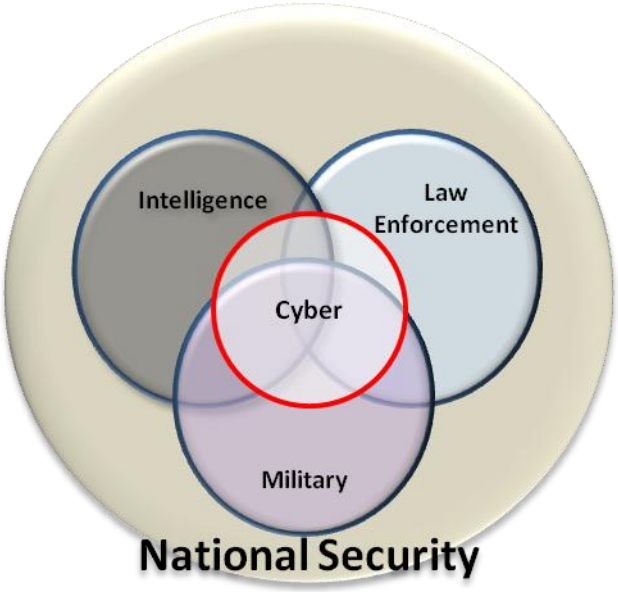
local agencies, along with both public and private spheres, into the information sharing movement.[60]

Convergence of all components of national security is in response to an ever-evolving threat. We must be prepared to wage war against potential enemy nation-states as we continue to wage war against activities such as illicit drugs and terror. The newest complication to the national security landscape is the advent of the cyber threat. The alarm is being increasingly sounded with respect to the cyber world.

> All the computer systems of the federal government are vulnerable to infiltration and disruption from hostile foreign governments or other foreign powers, international criminal enterprises, and lone hackers.
>
> And the concerns about network protection don't end at the outer bounds of the dot.mil or event the dot.gov cyber domains. We're also concerned about the serious national security threat to non-federal computer systems, including the networks of defense contractors working on sensitive projects, as well as the computers that control America's critical infrastructure, such as power plants and pipelines, electric grids, dams, water supply systems, air traffic control and rail transportation systems, banking systems and financial exchanges, and health care networks.[61]

All acknowledge that online threats must be addressed, but the lack of historical precedent creates a Gordian knot. Many questions are in debate and there are no easy answers. What is the proper role of the government in helping businesses respond to cyber security attacks? How much information should be shared between businesses and the government about online threats? How should cyber operations be reviewed, approved, and reported on in the executive branch? Are cyber operations governed by title 10 or title 50? Is the appropriate comparison for cyber operations to law of armed conflict or to criminal trespass? Upon deciding the proper framework, how is attribution to the correct perpetrator accomplished? How do we even distinguish between cyber defense, cyber attack, cyber exploitation, and traditional military activities? These

questions, plus more, need to be answered before the appropriate roles and authorities of the intelligence community, law enforcement, and the military in the cyber world can be definitively laid out and understood. For now, it is just taken for granted that all are involved and all are vulnerable. Accordingly, the cyber threat overlays all components of national security.



The So What of It All:

As has been shown, following the terrorist attacks on 9/11, the government was transformed, walls came down, and great strides were taken to increase integration and information sharing. One may wonder why there was ever resistance to this convergence in the first place. The simple fact is that when the authorities of all components of national security are utilized in unison, the amount of information collected and shared is increased exponentially. This increase is even more dramatic when combined with the advances in technological capabilities to collect and store

virtual mountains of data. Due to the nature of the threat of terrorism, much of that information is domestic. While increased information sharing creates risks to the government's obligation to protect sources and methods, this same sharing, at least with respect to data about U.S. persons, raises privacy and civil liberties concerns. "Some have argued that all these reforms to our intelligence, law enforcement and national security agencies have been at the cost of civil liberties and individual rights."[62]

The notion that fundamental changes in how security is provided would simultaneously be viewed as invasive of privacy was not unforeseen. The relationship between security and privacy is often described, apropos or not, as a balancing act. Accordingly, multiple measures were taken to make sure the proper balance would be struck and not swing too far in favor of security at the expense of privacy. For example, the Department of Homeland Security touts that it "has the first statutorily required privacy office of any federal agency, and the Department builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development."[63] Likewise, the Intelligence Reform and Terrorism Prevention Act of 2004 established the Civil Liberties Protection Officer (CLPO) for the Office of the Director of National Intelligence (DNI), along with such officers for other executive agencies and the Privacy and Civil Liberties Oversight Board.[64] The DNI's CLPO strives to ensure the protection of civil liberties and privacy is appropriately incorporated in the policies of the Intelligence Community as a whole.[65] Therefore, there are fleets of attorneys and supervisors, all sworn to uphold the Constitution, charged with obeying the mandate found in Executive Order 12333, "The United States Government has a solemn obligation, and shall continue in the conduct of

intelligence activities under this order, to protect fully the legal rights of all United States person, including freedoms, civil liberties, and privacy rights guaranteed by Federal law."[66] This is no easy task as that federal law mentioned above includes but is not limited to the First Amendment; Fourth Amendment; Privacy Act;[67] Electronic Communications Privacy Act (to include the Wiretap Act and the Stored Communications Act);[68] and FISA (to include the FISA Amendments Act) with its minimization procedures governing the acquisition, retention and dissemination of information concerning U.S. persons.[69]

The mere fact that positions have been created and multiple laws passed to protect civil liberties has not assuaged the fears of privacy advocates. There has been debate and dispute over virtually every step taken in the name of national security. To name but a small sampling, controversies have raged over the constitutionality of military commissions, the legality of the use of drones both as tools of domestic surveillance and targeted killing, and the propriety of the Total Information Awareness data-mining program. The list continues with what some label as scandals such as NSA's warrantless surveillance practice, the misuse of national security letters, and the controversy over the New York Police Department and CIA's alleged secret conspiracy to domestically spy on Muslims. As the list of controversies grows, it is readily apparent that a consensus view as to what is the proper balance between privacy and security may be unreachable. As one scholar points out, "You are either working to free all the criminals or you are an apologist for the fascist police state! This is not a field known for its conciliatory, nuanced unified approaches."[70] The debate has been framed with one side claiming that inarguably the government should provide for the common defense

but not at the sake of privacy, with the other side conceding that privacy should, of course, be protected, but not at the sake of security.

What is Reasonable?

The question is begged therefore, in light of the government's unified efforts to increase national security, what level of privacy is reasonable to expect? Traditionally, the Fourth Amendment's protection against unreasonable searches and seizures was founded in the common-law prohibition against physical trespass. This changed in 1967 with the Supreme Court's decision in *Katz v. United States*.[71] In Justice Harlan's concurrence, a new two-pronged standard was formulated to determine what protection would be afforded to people and their privacy interest: Does the person at issue have an actual subjective expectation of privacy, and is that expectation one that society is prepared to recognize as reasonable.[72] As technology advances, the applications of this test have become more and more complex and problematic. Recently, in *United States v. Jones*, the Supreme Court struggled with society's expectation of privacy in the context of governmental Global-Positioning-System (GPS) tracking of a vehicle's movements in public and on public thoroughfares.[73] Writing the opinion, Justice Scalia resorted to a trespass theory to censure the police's initial warrantless placement of the tracking device on the vehicle. Admittedly, Justice Scalia kicked the can down the road on the inevitable issue of when does electronic surveillance of one's movements in public constitutionally invade that person's privacy, stating, "We may have to grapple with these 'vexing problems' in some future cases where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here."[74] On the other hand, Justices Sotomayor and Alito, in

their concurrences, rushed forward and provided ample food for thought. Specifically, Justice Sotomayor questioned the "premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," claiming:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[75]

Justice Alito addressed the broader notion that technology changes the expectation of privacy, correspondingly changing the protection the Fourth Amendment provides as the *Katz* test hinges on the idea that only the expectations that society deems reasonable merit protection. "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[76]

Therefore, the United States finds itself in a very dynamic situation regarding its approach to national security. Walls have come down and the three components of law enforcement, intelligence, and the military are all taking advantage of overlapping authorities, advanced technological methods, and unprecedented information sharing. Simultaneously, America's views on privacy are evolving. The intersection of privacy and security is a vast and complex topic, but two relatively new concepts warrant brief mention.

First, the Third Party Doctrine, roughly stated, is that information voluntarily disclosed to third parties does not receive constitutional protection. In other words, there is no reasonable expectation of privacy in those communications. Justice

Sotomayor is not the only one to question the wisdom of this doctrine. Professor Murphy calls for increased third party protection by suggesting, "A reconstituted third-party doctrine might recognize that some disclosures are made in confidence, that there is value to such confidence, and that if the parties respect it, then the government should too." [77] While that idea sounds fairly innocuous, it oversteps by extending stout protection to information provided to any entity or confidante such as a "good ISP or best friend willing to resist government inquiries."[78] There is much debate about this occurring in academia, but one simple point seems to be overlooked. The law recognizes a very small group of communications so privileged and private as to be inviolable. This short list includes communications in the following relationships: attorney-client, husband-wife, and priest-penitent. Is society really ready to provide this same legal shield to relationships like internet service provider-web surfer?

Second, it is beyond cavil that society is becoming increasingly digitally connected and dependent. Our lives are out there on public display, digitally speaking. Undoubtedly, this technology boom provides great personal benefits and convenience. The flip side of that coin is that devices such as "cell phones, GPS devices, and web browsers generate massive amounts of digital information about us and make it available to others."[79] So, when the government avails itself of that information, claims abound of invasion of privacy, even if there would have been no violation if that same information had been collected by humans without the benefit of technology.[80] Counterintuitively, the expectation of privacy is no longer confined to private areas. In fact, Time Magazine lists the legal right to privacy in public spaces as one of the top 10 ideas that are changing our lives.[81] Some lament that it goes even further; that people

expect anonymity.[82] Like the third party doctrine debate, bright and ethical people land on all points of the spectrum. Even with that acknowledgement, it seems problematic to ideologically merge "private" and "public" through just sheer force of argument. For example, Justice Sotomayor claims a record of a person's public movements will contain data "the indisputably private nature of which takes little imagination to conjure."[83] How is doing something in public ever going to be indisputably private? Another example is the Rutherford Institute's claim that public surveillance reveals intimate details of personal lives.[84] Can the definitions of "intimate" and "personal" be logically stretched to include what a person does openly in public?

This evolving sense of privacy affects the war on terror. As FBI Director Robert Mueller commented after *Jones*, "It will inhibit our ability to use this [no expectation of privacy in public] in a number of surveillances where it has been tremendously beneficial. We have a number of people in the United States whom we could not indict, there is not probable cause to indict them or to arrest them who present a threat of terrorism. They may be up on the Internet, may have purchased a gun, but have taken no particular steps to take a terrorist act."[85] Interestingly, that wall between law enforcement and intelligence, so meticulously dismantled, could now be called upon to provide some of that desired protection to privacy. Justice Sotomayor spoke of the Fourth Amendment's goal to curb "police" power, and Justice Alito recognized that the privacy interest is different when "extraordinary offenses" are involved.[86] Justice Alito may have been referring to circumstances often involved in the war on terror. There is a foreign intelligence exception to the Fourth Amendment's warrant requirement.[87] This exception, rarely cited but nevertheless crucial, is analogous to the "special needs"

doctrine and revolves around the purpose of the collection. The Foreign Intelligence Surveillance Court of Review ruled:

> A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose. The prevention or apprehension of a terrorism suspect, for instance, is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection. In our view the more appropriate consideration is the programmatic purpose of the surveillances and whether – as in the special needs cases – that programmatic purpose involves some legitimate objective beyond ordinary crime control.[88]

Therefore, although information is shared and roles often overlap, it is still important to remember and respect a virtual wall that distinguishes between purposes. Privacy expectations should not be the same for law enforcement investigations as they are for intelligence collections. "The needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."[89] Different purposes require different standards; whereas law enforcement searches require belief of criminality, intelligence collection requires a link to a foreign power. It is not a far leap to suggest that the expectation of privacy may be required to shift in accordance with the purpose for which the privacy was infringed. After all, according to *Katz*, the expectation must be one that society is willing to protect. It is not unreasonable to argue that society could allow an ample expectation of privacy and assume some level of risk in the criminal arena while allowing much less privacy and assuming less risk when it comes to national security.

The war on terror changed every aspect of national security and its component parts of law enforcement, intelligence, and the military. Combating transnational criminals and state-sponsored terrorists in both the physical and cyber worlds requires

convergence, integration, and information sharing at unprecedented levels. In adapting its response to the current threat, America must still ensure hard-earned civil liberties. This becomes more complicated as the expectation of privacy evolves in the world of technological change. Therefore, relationships, authorities, procedures, and the law strive to keep pace.

Endnotes:

[1] *Posse Comitatus Act of 1878*, 18 United States Code Section 1385.

[2] *Restriction on Direct Participation by Military Personnel*, 10 United States Code Section 375.

[3] *Uniform Code of Military Justice*, 10 United States Code, Chapter 47, Section 802.

[4] *Ex Parte Milligan*, 71 U.S. 2 (1866).

[5] Ibid.

[6] Ibid., 124.

[7] International and Operational Law Department, *Law of War Deskbook*, (Charlottesville, VA: The United States Army Judge Advocate General's Legal Center and School, January 2010), 76.

[8] *Armed Forces*, 10 United States Code Title 10.

[9] *War and National Defense*, 50 United States Code Title 50.

[10] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal Online* 3 (2011): 86.

[11] Ibid.

[12] *National Security Act of 1947*, Public Law 235, 61 Stat. 496 (July 26, 1947*); Executive Order 12333: United States Intelligence Activities*, Federal Register Vol. 40, No. 235 (December 8, 1981, amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008)).

[13] Richard A. Best Jr., *Covert Action: Legislative Background and Possible Policy Questions* (Washington, DC: U.S. Library of Congress, Congressional Research Service, December 27, 2011).

[14] *National Security Act of 1947*, Public Law 235, 61 Stat. 496 (July 26, 1947), 50 United States Code Section 403-4a.

[15] U.S. Congress, House of Representatives, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century: Staff Study*, 104th Congress, June 5, 1996.

[16] *United States v. U.S. District Court*, 407 U.S. 297 (1972).

[17] James G. McAdams, III, "Foreign Intelligence Surveillance Act (FISA): An Overview," *Federal Law Enforcement Training Center Online* (March 2007): http://www.fletc.gov (accessed September 23, 2011).

[18] U.S. Congress, House of Representatives, Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century: Staff Study*, 104th Congress, June 5, 1996.

[19] Ibid.

[20] *Foreign Intelligence Surveillance Act of 1978*, Public Law 95-511, 92 Stat. 1783 (October 25, 1978).

[21] McAdams, "*Foreign Intelligence Surveillance Act (FISA): An Overview*."

[22] *Foreign Intelligence Surveillance Act of 1978*, Public Law 95-511, 92 Stat. 1783 (October 25, 1978), 50 United States Code Chapter 36.

[23] McAdams, "*Foreign Intelligence Surveillance Act (FISA): An Overview*."

[24] Ibid.

[25] National Commission on Terrorist Attacks upon the United States, Thomas H. Kean, and Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: W.W. Norton & Company, 2004).

[26] *Joint Resolution to Authorize the Use of United States Armed Forces Against Those Responsible for the Recent Attacks Launched Against the United States*, Public Law 107-40, 115 Stat. 224 and 225 (September 14, 2001).

[27] George J. Terwilliger III, Theodore Cooperstein, Shawn Gunnarson, Daniel Blumental, Robert Parker, "The War on Terrorism: Law Enforcement or National Security?" *The Federalist Society for Law and Public Policy Studies Online* (February 15, 2005): http://www.fed-soc.org (accessed September 27, 2011).

[28] *The United States Northern Command Home Page*, http://www.northcom.mil (accessed May 7, 2012).

[29] Robert Block and Gary Fields, "Is Military Creeping into Domestic Law Enforcement?" *Wall Street Journal*, March 9, 2004.

[30] Supervisory Special Agent Alan T. Ivy and Colonel Kenneth J. Hurst, *Formalizing Law Enforcement Procedures for DOD Units Conducting Combat Operations (Soldiers: The Street Cops of the 21st Century)*, Student Research Project (Quantico, VA: U.S. Marine Corps War College, 2007-2008), 1, citing Alexandra Zavis, "U.S. Troops Turn Police Investigators." *Los Angeles Times*, January 12, 2008).

[31] U.S. Congress, Senate, Senate Committee on the Judiciary, *Oversight of the U.S. Department of Justice*, 112th Cong., May 4, 2011, Questions for the Record.

[32] *Ex Parte Quirin*, 317 U.S. 1 (1942).

[33] *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004).

[34] *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006).

[35] *Boumediene v. Bush*, 553 U.S. 723 (2008).

[36] *Military Commissions Act of 2009*, Public Law 111-84, 123 Stat. 2190 (October 28, 2009).

[37] David S. Kris, "Law Enforcement as a Counterterrorism Tool," *Journal of National Security Law & Policy* 5, no. 1 (2011): 2.

[38] Mark Mazzetti and Eric Schmitt, "Obama's Pentagon and C.I.A. Picks Show Shift in How U.S. Fights," *New York Times*, April 28, 2011.

[39] Ibid.

[40] *Executive Order 13491: Ensuring Lawful Interrogations*, Federal Register Vol. 74, No. 16 (January 27, 2009).

[41] David Alvarez, "Militarization of CIA?" September 4, 2011, http://www.matisak.wordpress.com (accessed September 29, 2011).

[42] Ibid.

[43] Greg Miller, "Under Obama, an Emerging Global Apparatus for Drone Killing," *The Washington Post*, December 27, 2011.

[44] David Barrett, "Militarization of CIA?" September 4, 2011, http://www.matisak.wordpress.com (accessed September 29, 2011).

[45] P.W. Singer, "Essay: Double-Hatting Around the Law, The problem with Morphing Warrior, Spy and Civilian Roles," *Armed Forces Journal Online* (June 2010): http://www.armedforcesjournal.com (accessed September 23, 2011).

[46] Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 5 (2012): 539.

[47] Ibid., 542.

[48] Kean and Hamilton, *The 9/11 Commission Report*, 79.

[49] Ibid.

[50] Richard A. Best Jr., *Sharing Law Enforcement and Intelligence Information: The Congressional Role* (Washington, DC: U.S. Library of Congress, Congressional Research Service, February 13, 2007), 10.

[51] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Public Law 107-56, 115 Stat. 252 (October 26, 2001).

[52] Richard A. Best Jr., *Sharing Law Enforcement and Intelligence Information: The Congressional Role* (Washington, DC: U.S. Library of Congress, Congressional Research Service, February 13, 2007), 11.

[53] *In re Sealed Case 02-001*, 310 F.3d 717 (FISA Ct. Rev. 2002).

[54] McAdams, "*Foreign Intelligence Surveillance Act (FISA): An Overview*."

[55] National Security Preparedness Group, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* (Washington, DC: Bipartisan Policy Center, September, 2011), 6.

[56] *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-548, 118 Stat. 3638 (December 17, 2004).

[57] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Unclassified Version* (Washington, DC: March 31, 2005), Chapter Nine, Information Sharing.

[58] James B. Perrine, Verne H. Speirs, and Jonah J. Horwitz, "Fusion Centers and the Fourth Amendment: Application of the Exclusionary Rule in the Post-9/11 Age of Information Sharing," *Capital University Law Review* 38 (2010): 721, 734.

[59] Ibid., 735.

[60] Ibid.

[61] Steven G. Bradbury, "Keynote Address: The Developing Legal Framework for Defensive and Offensive Cyber Operations," *Harvard National Security Journal* 2 (2011).

[62] U.S. Congress, Senate, Senate Judiciary Committee, *Nominations to the Privacy and Civil Liberties Oversight Board, comments by Senator Charles Grassley (R-IA)* (April 18, 2012).

[63] Secretary Janet Napolitano, "Testimony before the United States Senate Committee on Homeland Security and Government Affairs," (September 13, 2011).

[64] *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, Public Law 108-548, 118 Stat. 3638 (December 17, 2004), Sections 1061 and 1062.

[65] ODNI Civil Liberties and Privacy Office, "Overview of ODNI Civil Liberties and Privacy Office," memorandum prepared March, 2011.

[66] *Executive Order 12333: United States Intelligence Activities*, Federal Register Vol. 40, No. 235 (December 8, 1981, amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008)).

[67] *Privacy Act of 1974*, Public Law 93-579, 88 Stat. 1896 (December 31, 1974).

[68] *Electronic Communications and Privacy Act of 1986*, Public Law 99-508, 100 Stat. 1848 (October 21, 1986).

[69] *Foreign Intelligence Surveillance Act of 1978*, Public Law 95-511, 92 Stat. 1783 (October 25, 1978), 50 United States Code Chapter 36.

[70] Erin Murphy, "The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr," *Berkeley Technology Law Journal* 24, (2009): 1240.

[71] *Katz v. United States*, 389 U.S. 347 (1967).

[72] Ibid.

[73] *United States v. Jones*, 565 U.S. ___ (2012).

[74] Ibid.

[75] Ibid.

[76] Ibid.

[77] Murphy, "The Case Against the Case for Third-Party Doctrine," 1252.

[78] Ibid.

[79] Massimo Calabresi, "Privacy in Public," *Time*, March 12, 2012, 81.

[80] Carrie Johnson, "FBI Still Struggling With Supreme Court's GPS Ruling," *National Public Radio Online* (March 21, 2012): http://www.npr.org (accessed March 21, 2012).

[81] Calabresi, "Privacy in Public," 80.

[82] Mike Nizza, "An Intelligence Official's Privacy Proposal," *New York Times*, November 12, 2007.

[83] *United States v. Jones*, 565 U.S. ___ (2012).

[84] John W. Whitehead, "U.S. v. Jones: Where Privacy, Technology, and the Constitution Collide," *The Huffington Post Online*, October 10, 2011, http://www.huffingtonpost.com (accessed March 21, 2012).

[85] Johnson, "FBI Still Struggling With Supreme Court's GPS Ruling."

[86] *United States v. Jones*, 565 U.S. ___ (2012).

[87] *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973).

[88] *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008).

[89] *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980).