

# OFFICE OF CONGRESSIONAL AFFAIRS

DATE: 7 January 2002

TO: Mr. Andrew Napoli  
Office of The Honorable Christopher H. Smith

PHONE: (202) 225-3765

FAX NO.: (202) 225-7768

-----  
FROM:

A rectangular box with a thin black border, used to redact the name of the sender.

(b)(3)

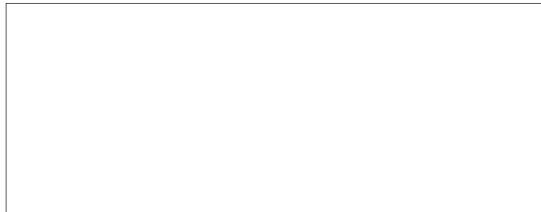
PHONE:

FAX NO.

COMMENTS:

For your information, I have enclosed a portion of an unclassified address by former General Counsel Robert M. McNamara, Jr., before the ABA Standing Committee on Law and National Security on 1 December 2000. The document provides useful background information on unauthorized disclosure legislation and the damage caused by unauthorized disclosures. As required by Sec. 310 of H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002, the Attorney General, in consultation with the DCI and other heads of U.S. government departments and agencies, is currently conducting a review of the laws and regulations governing unauthorized disclosures and whether modifications to law or regulation are required to prevent future unauthorized disclosures.

I hope this information is useful to Representative Smith in responding to his constituents. If you need additional information or would like to speak with me further, feel free to call me on

A rectangular box with a thin black border, used to redact a phone number.

(b)(3)

NO. OF PAGES PLUS COVER: 5

TTI OFFICE OF PUBLIC AFF

DATE	TIME	ADDRESS	MODE	TIME	PAGE RESULT	PERS. NAME	FILE
JAN. 7.	3:35PM	202 225 7768	TES	2'29"	P. 5 OK		820

# : BATCH  
M : MEMORY  
S : STANDARD

C : CONFIDENTIAL  
L : SEND LATER  
D : DETAIL

\$ : TRANSFER  
@ : FORWARDING  
F : FINE

P : POLLING  
E : ECM  
> : REDUCTION

National Security Law in a Changing World:  
The Tenth Annual Review of the Field

American Bar Association  
Standing Committee on Law and National Security

Capital Hilton  
Washington, D.C.  
1-2 December 2000

Panel I: Round Table Discussion

(1 December 2000)

*Survey of New Developments In National Security Law: Executive  
Branch Perspectives*

(Moderator: Elizabeth Rindskopf Parker. Panelists:  
Jane Dalton JCS, Bob Dietz NSA GC, Bob McNamara CIA GC,  
Larry Parkinson FBI GC, James Thessin DOS)

Introduction

Thank you, Elizabeth. I appreciate your warm introduction, and am happy to serve on this panel again with my esteemed colleagues.

I have been General Counsel of the Central Intelligence Agency (CIA) for three years now and the issues we face remain as challenging, if not more so, as the day I arrived. Some of the issues we discussed last year--such as intelligence collection in the information age, or intelligence support to war crimes tribunals--continue to occupy much of our time and energy. Meanwhile, additional issues have come to the forefront, including how best to address the continuing problems of unauthorized leaks of classified information, and the use of intelligence to support United States law enforcement activities abroad.

We attorneys, like the intelligence agencies we represent, must be responsive to the enduring challenges and creative in addressing the new ones. We have to be willing to move beyond the "tried and true" to get to solutions that will work in the

new millennium, but maintain as a constant the rule of law.

I would like to briefly discuss four issues of concern, namely:

How to address the continuing and serious problem of leaks of classified information

How best to support international law enforcement within the boundaries of our own authorities

How to employ new collection technologies under the law in the Internet era, and

How best to provide support to international war crimes tribunals, without needlessly risking our sources or methods in the course of multinational litigation.

### Leaks

As you know, on November 4th the President vetoed the FY 2001 Intelligence Authorization Act, because of what he termed "one badly flawed provision" on leaks. The leaks legislation was intended to stem the tide of unauthorized leaks of classified information that have caused serious damage to both technical and human sources.

Over the last two years, CIA's Center for Security has opened more than 150 investigations of alleged leaks. Although I cannot cite specific examples, let me assure you that the lives of covert sources have been placed in jeopardy and the Intelligence Community's ability to collect vital intelligence has been seriously impaired by these leaks--many of which are simply not covered by the existing espionage laws.

As the President's veto statement made clear, he viewed the provision as overbroad and one which would unnecessarily chill legitimate activities. In large part, the President's concerns were reflected by critics of the draft legislation who derided the proposal as an attempt to enshrine into American law an Official Secrets Act, and who claimed that such a statute was unnecessary in light of the current espionage laws. Many commentators also raised the specter that the Government could subpoena a reporter in an attempt to discover the source of the leak, and asserted that the provision would somehow unconstitutionally infringe the freedom of the press.

The Department of Justice (DoJ) had worked closely with the Intelligence Committees and the Intelligence Community, including the National Security Council and Department of State, to fashion a narrowly constructed prohibition. DoJ reviewed the final proposal and determined that it was constitutional since it was directed only at Government employees and contractors, and there is no constitutional right of an employee or contractor to breach his trust and to leak classified information.

With respect to the issue of press freedom, there exists current authority to subpoena reporters during an investigation under 18 U.S.C. §793, however it is long-standing DoJ policy to prevent the issue of a subpoena to a reporter without specific approval from the Attorney General--and such an approval has never been granted.

In the meantime, the existing laws by which the Government may deter and punish leakers who put lives at risk remain limited. The simple fact is that existing law protects only information relating to the national defense, cryptographic information, and the identities of intelligence officers and agents. But information regarding some covert action programs, our liaison relationships with foreign governments, intelligence on narcotics trafficking and money-laundering, and our counterintelligence capabilities are not protected by the terms of the existing criminal statutes.

Administrative sanctions are not the answer. Administrative sanctions--such as firing, reprimand or leave without pay--may be imposed upon current government employees if they are found to have leaked classified information. Those avenues, however, are not available to discipline former employees or contractors.

At most, an individual's continued access to classified information may be withdrawn--a deterrent to be sure, but an insufficient one, especially when the leak jeopardizes the life of an asset, compromises a sensitive foreign intelligence relationship, or results in the loss of a critical intelligence capability.

Clearly, any consensus on this issue will be hard to achieve, but we must work together to find a workable solution. Some have suggested that we limit any new statute to protect only Sensitive Compartmented Information, which is clearly the most closely held set of information, but any statute so limited would exclude, for example, information derived from certain liaison

relationships with foreign governments, details on how we establish and run CIA proprietary companies, information on sensitive counter-intelligence targets--each of which, if disclosed, still can damage our ability to collect foreign intelligence which is needed by the policymakers and the war fighters to do their jobs.

In the course of discussions on the proposed statute, some have suggested imposing a requirement that the Government must prove actual harm from a disclosure in order to obtain a conviction. I do not support that approach, for it seems to me that the result would be to require the Government to disclose even more classified information in order to prove its case, thereby compounding the damage from the original leak. This approach would also encourage defendants to attempt a "graymail" defense. In other situations, it may not be possible immediately to quantify the harm or to assess the damage because of the long-term effect of the leak itself.

As an alternative to a requirement that the Government show harm from a specific disclosure, the suggestion has been made that the Government simply establish that the defendant intended by the disclosure to harm the US. But intent to cause harm is not really the issue in these types of leaks--it is the fact that regardless of intent, these leaks, simply put, can get our sources killed or negate our capabilities. It is little solace to the families of those assets, or to our national intelligence effort, that the leaker, who often is far removed from any appreciation of the consequences of his or her actions, did not intend that result.

As I said earlier, we need to find a solution that both protects properly classified information from unlawful disclosure and ensures that the press remains free and robust. The compromise of either of these critical values is not an acceptable solution.

#### International Law Enforcement

As the world shrinks, the reach of criminal law systems of both nations and international organizations has grown. One trend that we expect to continue is the increase in extraterritorial application of US criminal laws. For example, the 1996 Antiterrorism and Effective Death Penalty Act criminalized certain terrorist actions no matter where in the world they occur.

And other nations, of course, have enacted criminal laws relating to terrorist attacks by or against their own citizens. Our intelligence activities in this area require coordination and cooperation with the various Federal law enforcement agencies, especially those like the FBI that have both law enforcement and intelligence components.

A prime example of the growing convergence of foreign intelligence and international law enforcement is the work of the two communities in the field of counterterrorism. As you know, (b)(1) (b)(3)

An instance in which the interaction of law enforcement and intelligence operations became critical was the period surrounding the Millennium celebrations in January of this year. Just as in years past when the Olympic Games were an obvious terrorist target, the Millennium celebrations could have generated huge audiences for terrorist attacks. Many threats against US citizens and interests arose around the world during that time.

One individual was arrested by US Customs officials while crossing the US border between Canada and the state of Washington with bomb-making materials in his car. Others were arrested in the Middle East by Jordan, which subsequently announced that the persons in custody had planned attacks on popular tourist sites there. Additional information about threats came from numerous individual informants volunteering their knowledge.

In all these cases, the collection and evaluation of intelligence had to be done in coordination with law enforcement interests and authorities. The intelligence mission was to gather and provide timely warning information to US policy makers

so that future attacks could be prevented, disrupted, or mitigated. In addition to those goals, the law enforcement mission sought to capture and subject to criminal trial those persons conspiring to or carrying out terrorist attacks. This required additional efforts to preserve information for possible use as evidence in future prosecutions.

In these areas and others where the intelligence and law enforcement communities have had to work together to acquire information, particularly overseas, we have had to ask ourselves whether information is potential evidence or does it have value as intelligence? More often now, the answer is both. And it is critical that the information be exploited for both purposes--we will look to prosecute past criminal acts and foil future ones.

Fortunately, we now understand that and work to preserve the value of what we collect to satisfy both governmental needs. Although I cannot comment in detail about the current investigation into the attack on the USS COLE in Aden harbor, I can say that the same considerations are in play, as they were during the bombings of the east African embassies in 1998.

As you all know, documentary evidence requires use of originals. Intelligence analysis does not. You can see that in this instance the US Government can preserve an original document for possible evidentiary use while permitting the intelligence community to use a duplicate to satisfy intelligence needs. While this may seem like an obvious solution, I can tell you that just a few short years ago, this duality was not easily satisfied. So we have come a long way.

Countering foreign terrorists has both intelligence and law enforcement components. We do have some statutory schemes that erect a legal line between the two, such as the Foreign Intelligence Surveillance Act. In an increasing number of activities overseas, however, the complementary and overlapping nature of the efforts are striking. Although the National Security Act prohibits CIA from exercising any law enforcement powers or internal security functions, it may support law enforcement activities of other Federal agencies by providing intelligence, expert personnel, and specialized equipment.

The FBI is a law enforcement agency. Yet it has a full division devoted to counterterrorism that is both an avid consumer and producer of foreign intelligence information. The Millennium celebrations showed that international terrorist



threats do not fall into neat categories of domestic or foreign, law enforcement or intelligence, diplomatic or military. Countering terrorist threats is thus a seamless endeavor for much of the US government.

### Intelligence Collection in the Internet Age

Another issue that we are grappling with is whether the legal and regulatory framework developed in the late 1970's and early 1980's is sufficiently flexible to address foreign intelligence issues that arise in the context of the new global information infrastructure.

For years, the dual criteria of geography and status were sufficient to dictate the rules and differentiate the authorities. Is the person inside or outside the US; is he a US person or not? As an example, the CIA lawfully may collect foreign intelligence information about non-US persons overseas. At the same time, we are prohibited by law from engaging in technical surveillance within the United States or collecting against US persons overseas unless the Attorney General has approved.

In the relatively recent past, it was fairly easy to apply these rules, by determining where the target was located and where the information would be collected. But this is not always the case in today's environment--electrons flow seamlessly across borders; user identities and nationalities are often cloaked; technical attacks against US computers may be made from undetermined locations anywhere in the world--or the US.

Overseas attackers have been known to establish an illicit presence on US networks and launch attacks from overseas locations, but masquerade as if they are attacking from sites in the United States. Responding to these challenges can be similarly complex, yet our statutes and regulations implementing the Fourth Amendment's protections against unreasonable searches and seizures are still driven by common law concepts developed in an age when all communications relied on telephone lines and in which geography is a critical component.

Complicating the issue of legal authority based upon location is the fact that cyber attacks against the US simultaneously raise issues of law enforcement and foreign intelligence. These issues are not purely theoretical. Several years ago, the Clinton administration was seriously considering

authorizing a military response to certain actions undertaken by Iraq. As possible US military responses were being discussed in the media, a significant number of unclassified Department of Defense (DoD) sites were subjected to a coordinated series of cyberattacks. A significant number of these attacks appeared to originate from an internet service provider in the Middle East.

DoD obviously was concerned about its ability to wage warfare, and explored actions it legally could take to identify and take action against the perpetrators. DoJ and the FBI wanted to preserve the ability to prosecute the cyberattackers for what was a clear violation of US law. The fact pattern also indicated the possibility of state sponsorship. In that particular case, the computer network defense community, led by DoD computer incident response teams and by the DoJ, was able to trace the attacks back to northern California.

The perpetrators were teenagers who suffered from a severe case of bad timing. Despite the initial concerns, this particular case remained almost exclusively a law enforcement activity. However, it should be emphasized that not all attacks are so benign; not all attackers are as easily identified; and not all such activities fall so clearly within law enforcement's exclusive jurisdiction.

Not only do these issues require effective deconfliction with law enforcement, but from an Intelligence Community perspective, it matters greatly whether a US system is under attack by an organized foreign sponsored collection team, or by computer savvy teenagers in the US. It is important to remember that, even in this emerging area, we remain a government of limited powers. The CIA specifically is not authorized to engage in law enforcement activities.

As we work through these issues in today's telecommunications environment, lawyers in the intelligence community are developing close working relationship across the community. Lawyers involved in this area also are working closely with the operators and are becoming much more knowledgeable on the way the global information infrastructure works. The attorneys in my office, in close coordination with the FBI's National Infrastructure Protection Center (NIPC), the Department of Justice, and attorneys throughout the Intelligence Community and DoD, are grappling with these issues on a daily basis.

In addition to playing a role in protecting the US

infrastructure, we also continue to have as our primary mission the collection of foreign intelligence information that is of value to high-level policy makers. The information explosion has made collection of intelligence information much more complicated. The sheer volume of information presents a daunting challenge from both the collection and the processing point of view.

Our guiding standard continues to be Executive Order 12333 and implementing regulations that have been approved by the Attorney General. This regulatory framework governs the way in which the intelligence community collects, processes and retains information that may contain incidentally collected US person information. To date, these guidelines have proven sufficiently flexible that they remain relevant and useful notwithstanding the changed global telecommunications environment. These remain cutting-edge issues that will continue to make life interesting and challenging for intelligence community lawyers for the foreseeable future.

#### Support to International Tribunals

As I indicated the last two years, as international tribunals continue to be created, we anticipate that more demands will be made for intelligence support. Already there are tribunals for the former Yugoslavia and Rwanda, the Scots are trying the Lockerbie defendants as we speak, and although the United States has not acceded, there soon will be an International Criminal Court. There is talk of tribunals to address war crimes issues in Iraq, Thailand, Sierra Leone, Cambodia, and Indonesia.

The Intelligence Community's support to the US Government effort in identifying the perpetrators of war crimes and other atrocities in Bosnia, Kosovo, and Rwanda has been significant. There has also been an increase in requests for information which would assist the War Crimes Tribunals in bringing persons indicted for war crimes to justice. Generally, these requests for intelligence support are of three types: requests for background information, requests for leads, and requests for testimony and or evidence.

The nature of the requests also has changed: we now are being asked to authorize the use of sensitive intelligence information for trial, sometimes in the form of unclassified products derived from our technical collection systems. We have

worked hard to solve the technical problems of creating products that are both useful to the Tribunal and do not reveal intelligence sources and methods. In this effort, we have also had to address equally difficult legal problems. As much as we need to support these tribunals, we may not enjoy the same protections for our sources and methods in those settings as we do in American courts.

While we continue to look for intelligence information that will aid in the indictment and prosecution of war criminals, we also are required by law to ensure that sources and methods are protected from unlawful disclosure. All of this is being done within the legal environment of Tribunal's rules of evidence and practice, which, while on the one hand promise confidentiality, also guarantee that certain information will be disclosed to the defendants. That said, both the Scottish panel trying the Lockerbie defendants, and the International Criminal Tribunal of the former Yugoslavia (ICTY), have developed processes and procedures to protect intelligence information. We are impressed by these efforts, but note that their true effectiveness remains to be determined.

Perhaps the most remarkable example of CIA support to a foreign criminal tribunal is that which CIA provided to the Scottish prosecution of the two Libyan intelligence officers on trial for the December 1988 bombing of Pan Am Flight 103 over Lockerbie. Because the case is ongoing, my comments have to be a bit limited.

Colin Boyd, the Lord Advocate of Scotland, has informed me that Scottish law frowns greatly on commentary on the evidence in a trial before that trial is concluded. I intend to honor his wishes. The Agency has invested too much time and effort to this case to do otherwise. Nevertheless, I can give you some detail of what I believe to be extraordinary support the CIA has provided in this case.

Just two weeks ago, the prosecution in the trial rested its case. The CIA made available to the Scottish prosecution, dozens of classified operational cables, several classified CIA laboratory reports, and several officers as witnesses. The laboratory reports and many of the cables were redacted for introduction as evidence or disclosed to the defense. Several officers and a former source have testified to date. Because of the legal and operational security complexities, CIA assigned [redacted] lawyers and a senior Directorate of Operations officer to support the case. All this is unprecedented.

(b)(3)

The "Law of the Tribunal" is developing, and not always in a comfortable direction. One case before the Yugoslav war crimes tribunal is of particular interest because it raises a number of critical issues. This last summer, the Trial Chamber issued a very troubling opinion that would extend the Tribunal's jurisdiction to organizations such as NATO and the UN Stabilization Force (SFOR), would compel the production of information by SFOR and its member States concerning the apprehension of persons indicted for war crimes, and would compel the testimony of senior US military personnel in their personal capacity for matters related to their service with SFOR.

In the last year the US also had a very instructive experience with a truly independent prosecutor. When allegations were made against the NATO bombing campaign in Yugoslavia, we were in the unusual and uncomfortable position of having to wait while Carla Del Ponte, the ICTY prosecutor, conducted a preliminary inquiry of the allegations. Fortunately, Mme. Del Ponte concluded that no further action was required by her office. Nonetheless, this incident was instructive and may forecast our relationship with other international tribunals, such as the International Criminal Court.

Our intelligence is also used in parallel public diplomatic efforts on war crimes issues. When intelligence is used publicly, our policymakers must be cognizant of the impact of the public use of intelligence on war crimes prosecutions. For instance, using intelligence information to publicize suspected war crimes may, if the public release is premature, cause the destruction of the very evidence necessary to prosecute those who committed these crimes.

Finally, I should add a word of caution. Prosecutors, whether domestic, foreign or international, have to be sensitive to the fact that intelligence may not provide the evidence they seek and that intelligence should not be treated as "ordinary evidence". Although much of our intelligence may support individual prosecutions, it remains the case that in general our intelligence collection is designed to learn the capabilities and intentions of nations, groups, or elements, particularly those potentially hostile to the US.

Generally speaking, intelligence collection is not specifically tuned to the collection of information which would help determine individual culpability. Collection on issues of individual culpability may occur as a by-product of our

intelligence collection efforts, but not as their primary focus. Also, we often do not have the full story. Consequently, our analysis and conclusions are often based on hypothesis--supported by facts. Although the bases for our conclusions may be sufficient for a US policymaker to make a decision, they may fall somewhat short of the standard of proof required in a criminal case.

#### Conclusion

These issues clearly pose substantial challenges. There are no easy solutions, and if there were, this job would be much less interesting.