Testimony of
Kim Taipale, Executive Director
Center for Advanced Studies in Science and Technology Policy
www.advancedstudies.com

Before the
House Permanent Select Committee on Intelligence
United States House of Representatives
July 19, 2006

Mr. Chairman Hoekstra, Ranking Member Harman, and Members of the Committee: Thank you for the opportunity to testify today on potential legislation to amend the Foreign Intelligence Surveillance Act (FISA) and related matters.

My name is Kim Taipale. I am the executive director of the Center for Advanced Studies in Science and Technology Policy, an independent, non-partisan research organization focused on information, technology, and national security issues. I am also a senior fellow at the World Policy Institute at the New School and an adjunct professor of law at New York Law School.

By way of further identification, I also serve on the Markle Task Force on National Security in the Information Age, and on the Science and Engineering for National Security Advisory Board at the Heritage Foundation. Of course, the opinions expressed here today are my own and do not represent the views of any of these organizations.

My testimony today is in two parts. The first part discusses some of the inadequacies of the current law to address certain foreign intelligence surveillance needs and, in particular, recent technology developments. The second part offers my view on some of the possible legislative solutions to these deficiencies and related issues, including a very brief review of some the Constitutional, legal, and policy issues involved.

My formal testimony does not address directly the existing controversy over whether the President currently has inherent or statutory authority to approve the National Security Agency (NSA) Terrorist Surveillance Program or any other specific operational program – an issue on which I have not taken a public position.

Nevertheless, I would like to make two comments relating to that issue before proceeding:

- First, it seems clear that even the most strident opponents of the current program concede the need to identify and monitor the communications of terrorists and stop them before they can act, and

- Second, it seems clear that even the most strident supporters of the program concede that an institutional clash between two branches of government – regardless of the outcome – is not the best way forward, thus, a legislative solution is preferable.

Therefore, in the debate over *who* should have the authority to authorize and oversight these intelligence gathering programs, we cannot lose sight of the fact that *someone* must – and, for the reasons described below, the existing mechanisms are inadequate.

A final comment before proceeding – and this comment runs the risk of becoming cliché in the current debate – security (in this case, enabling appropriate foreign intelligence surveillance) and civil liberties (in this case, the privacy interests of U.S. citizens, and others, in their communications) are not dichotomous rivals to be traded one for another in a zero-sum game but are dual obligations of a liberal democracy that must each be maximized within the constraints of the other. Security without liberty is untenable, yet liberty is not possible without security.

FISA is inadequate.

Although I intend in my testimony today to focus in particular on how FISA is challenged by certain technology developments – including: the transition from circuit-based to packet-based communications; the globalization of communications infrastructure; and, most especially, the development of automated monitoring techniques, including data mining and link or traffic analysis – the suggestion that FISA procedures are inadequate to encompass certain aspects of foreign intelligence surveillance is not new, nor unique to these technical developments.

Testifying before the Church Committee in 1975, then-Attorney General Edward Levi suggested that FISA should include provisions for the approval of "programs of surveillance" in foreign intelligence situations where "by [their] nature [they do] not have specifically predetermined targets" and where "the efficiency of a warrant requirement would [therefore] be minimal." However, Congress passed FISA in 1978 without including any provisions for such programmatic approvals.

In a recent essay, Judge Richard A. Posner observed that FISA "retains value as a framework for monitoring the communications of known terrorists, but it is hopeless as a framework for detecting terrorists. [FISA] requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist." He goes on to point out that FISA's limitations are "borrowed from law enforcement" in which "crimes are committed, there are usually suspects, and electronic surveillance can be used to nail

them." But, in counterterrorism intelligence the need is the inverse — you don't always have suspects and you may need electronic surveillance to find them.

In my view, by not including provisions for programmatic approvals, FISA simply did not anticipate the development of global communication networks or advanced technical methods for intelligence gathering that themselves can help allocate law enforcement or national security resources toward more likely targets by monitoring communications and revealing evidence of organization, relationships, or other relevant patterns of behavior indicative of potential threats— that is, technologies that can help develop reasonable suspicion for further investigation. Further, it did not anticipate the national security need to employ these technologies to pick out "signals of interest" — things like al Qa'ida communications — from a sea of global communications.

FISA provides a cumbersome mechanism requiring individual application to the FISA court for authorization to target a specific individual or source based on a prior showing of a connection to a foreign power or foreign terrorist group. Although FISA permits such applications to be made after the fact in certain cases, it does not provide a mechanism for programmatic pre-approval of technical methods like automated data or link analysis, filtering, or other electronic surveillance that may be the very method necessary for uncovering such a connection in the first place. As General Hayden has testified, "FISA was built for long-term coverage against known agents of an enemy power" but the current need is to employ technical means to help "detect and prevent" future terrorist activity.

Thus, as I will discuss in the second part of my testimony, proposed legislation such as the Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act ("LISTEN Act") that are intended simply to streamline the existing FISA procedures address only half of the problem. Unfortunately, it is not just the procedural encumbrances of FISA that need reform but the rigid singular statutory requirement for showing probable cause of a connection to a foreign power prior to engaging in any electronic surveillance that needs to be addressed. And, it should be emphasized, as discussed below, that this inflexible standard is a FISA-created statutory constraint, not a Constitutional requirement.

From circuit-based to packet-based communication networks.

To understand the need for applying automated data analysis technologies to foreign intelligence surveillance requires not just recognizing the vast global communications volumes potentially subject to monitoring — imagine for a moment the capture of an al Qa'ida laptop containing hundreds or thousands of phone numbers or email addresses — but also an understanding of the nature of modern communications networks.

Thirty years ago when FISA was being drafted it made sense to speak exclusively about the interception of a targeted communication — one in which there were usually two known ends and a dedicated ("circuit-based") communication channel that could be "tapped." In modern "packet-based" networks, however, data and increasingly voice

communications are broken up into discrete packets that travel along independent routes between point of origin and destination where these fragments are then reassembled into the original whole message. Not only is there no longer a dedicated circuit, but individual packets from the same communication may take completely different paths to their destination. To intercept these kinds of communications, filters ("packet-sniffers") and search strategies are deployed at various communication nodes to scan and filter all passing traffic with the hope of finding and extracting those packets of interest and reassembling them into a coherent message. Even targeting a specific message from a known sender may require intercepting (i.e., scanning and filtering) the entire communications flow at one or more particular nodes. Were FISA to be applied strictly according to its terms prior to any "electronic surveillance" of foreign communication flows passing through the U.S. or where there is a substantial likelihood of intercepting U.S. persons, then no automated monitoring of any kind could occur.

The globalization of communications.

A further problem arises because FISA is triggered by foreign intelligence collection conducted "within the United States" or against "U.S. persons." Advances in information technology together with the borderless nature of terrorist threats and global communications has made place-of-collection and U.S. personhood an increasingly unworkable basis for controlling the collection of intelligence.

Indeed, because of packet-based communication technologies, like VoIP, and the use of proxy servers, it may no longer even be technically possible to determine exactly when a communication is taking place "within the United States" and no practical means exists to determine if a particular participant is a U.S. person or not until after further investigation. Additionally, the routing of significant amounts of international communications traffic through communications nodes physically located in the U.S. further complicates the interception of even erstwhile “wholly-foreign” communications. FISA does not account for these problems.

More importantly, whether or not a communication takes place within the United States or involves U.S. persons is an arbitrary distinction in determining whether the communication has “foreign intelligence value” and, therefore, whether it is a legitimate subject of foreign intelligence surveillance.

Automated analysis: data mining and link or traffic analysis.

Especially challenging under existing FISA procedures is the use of automated screening methods that can monitor data flows to uncover terrorist connections or terrorist communication channels without human beings ever looking at anybody's emails or listening in on their phone calls. Only when the computer identifies suspicious connections or information do humans get involved.

It is not possible in an open hearing to explore all the different analysis techniques that can be applied to the monitoring of terrorist communications but two generic examples illustrate the range of activity possible: content filtering and link or traffic analysis.

Content filtering is used to search for the occurrence of particular words or language combinations that may be indicative of terrorist communications. Link analysis involves determining who is talking to whom. And, traffic analysis is the examination of traffic patterns — message lengths, frequency, paths, etc. — of communications without focusing on the content of the message. Link and traffic analysis can reveal patterns of organization or suspicious links, thus, help identify organizations or groups as well as key people within or affiliated with them.

The issue with automated monitoring is under what conditions such monitoring itself can provide the reasonable predicate to allocate additional investigative resources for follow up investigation.

'Programs of surveillance' are not general warrants.

It is important to point out that I am not suggesting that these technologies should be (or are being) used in an undirected fashion in the manner of a general warrant to examine all communication flows to look for general indicia of "suspicious behavior." Indeed, they should not be employed as a general method for finding terrorists by monitoring all global communications with no starting point, nor for determining guilt or innocence.

Rather, they are powerful tools to help better allocate law enforcement and security resources to more likely targets. What is needed is a mechanism for programmatic approval whereby these techniques can be applied in the first instance against known or reasonably suspected foreign terrorist communication sources — that is, against legitimate foreign intelligence targets not subject to FISA and not requiring a warrant — and then used to automate the process of looking for connections, relationships, and patterns for further follow-up investigation.

If the initial process identifies potentially suspicious connections to or from legitimate foreign intelligence targets — including, for example, U.S. persons or sources communicating with known or suspected terrorists or through known or suspected terrorist communication channels — then some additional appropriately authorized monitoring or follow-up investigation (including analysis, monitoring, or additional circumscribed electronic surveillance of those communications) should be permitted in order to determine if that initial "suspicion" is justified.

The problem with FISA is that it contemplates only a single binary threshold for authorizing any electronic interception within the U.S. or targeting U.S. persons — probable cause that the target is an agent of a foreign power. Thus, for example, where a communication that triggers FISA (i.e., involves a U.S. person or source) is intercepted collateral to a legitimate foreign intelligence intercept it must be "minimized" (essentially not followed up on) unless its "foreign intelligence value" is immediately apparent or if

probable cause exists *prima facie* to target the new connection. Unfortunately, a single initial contact with even a known terrorist may not be legally sufficient to meet the existing probable cause standard of FISA yet may have significant "foreign intelligence value" requiring follow up investigation. I believe that it is specifically this situation that Gen. Hayden has referred to as "soft triggers" in the context of the current NSA program.

What is needed, I believe, is the electronic surveillance equivalent of a *Terry* stop — the Constitutionally permissible procedure under which a police officer can briefly detain someone for questioning and conduct a limited pat-down search if they have "reasonable suspicion" to believe that the person may be involved in a crime (*see* Terry v. Ohio, 392 U.S. 1 (1968)). In the case of electronic surveillance, this would permit an authorized period for follow up monitoring or investigation of initial suspicion derived from automated monitoring (or otherwise developed collateral to a legitimate foreign intelligence intercept).

This follow up investigation may require limited electronic surveillance of U.S. persons or within the U.S. predicated on some reasonable threshold indicia of suspicion. If ongoing suspicion is not justified on follow-up analysis or surveillance, monitoring would be discontinued and normal minimization procedures would be triggered, however, if suspicion is reasonably justified then monitoring could continue under the programmatic approval for some limited further period to determine if standard statutory probable cause can be established. If there is probable cause to suspect that the target is actively engaged in terrorism or is an agent of a foreign terrorist group, then a regular FISA warrant can be sought to target that U.S. person or source for full surveillance.

Based on published reports and public statements by intelligence officials responsible for the NSA Terrorist Surveillance Program it is my belief that this indeed describes generally the procedures that the current program is following. I refer here specifically to Gen. Hayden's address to the National Press Club on January 23, 2006.

What is needed then is a statutory mechanism with appropriate checks and balances for authorizing and oversighting such methods so that legitimate foreign intelligence can be exploited and further threats identified for follow up investigation. With programmatic approval of initial monitoring and a circumscribed procedure for limited follow up investigation, existing FISA warrant procedures could then be followed for targeted monitoring of identified U.S. persons or sources in those cases where the results of the initial monitoring and follow up enquiry determined probable cause.

In the next part of my testimony I comment briefly on some of the Constitutional, legal, and policy issues involved in amending FISA to provide for such authorization and oversight.

Possible Legislative Solutions

It is not possible — nor do I intend — in the time remaining to fully expose all of the Constitutional and statutory issues involved in amending FISA or that may govern

electronic surveillance. Nor, is it possible to fully comment in detail on all of the currently proposed draft bills and their detailed provisions.

Rather, I would like to focus the Committee's attention on a few issues that, in my view, are generally not parsed with sufficient nuance in the public debate, and to suggest how those issues may be implicated by various legislative approaches, including the various draft bills in circulation.

Constitutional Issues

Before I begin discussing the Constitutional issues, I would point out that support for much of what I am about to say can be found in the testimony of Attorney General Edward Levi before the Church Committee in 1975, and in the testimony of David S. Kris, a former senior DOJ official with significant expertise in this area, in his recent testimony before the Senate Judiciary Committee on March 28, 2006. I would urge the Committee to review those testimonies.

I would like to make three simple points about the Constitutional framework within which any legislative solution will be crafted. I believe that each of these points is subject to both popular misunderstanding and frequent misstatement:

- first, the Fourth Amendment does not prohibit warrantless searches, including warrantless electronic surveillance, under appropriate circumstances;

- second, probable cause is not a static requirement but is measured by the reasonableness of the search in the particular context, including the Government interest to be served; and

- third, the particularity requirement of the Fourth Amendment does not, in fact, always require *individualized* suspicion.

Thus, there is no Constitutional prohibition to a carefully crafted legislative solution that would authorize programmatic approval of electronic surveillance programs permitting limited electronic surveillance of U.S. persons or within the U.S. for foreign intelligence purposes without requiring a traditional warrant based on individualized probable cause. Further, permitting such programs may actually be preferable — and, ultimately, less intrusive to civil liberties — than alternative methods, for example, requiring physical surveillance to independently establish probable cause following a determination of reasonable suspicion collateral to a legitimate foreign intelligence intercept.

The following discussion is not intended to be a comprehensive Constitutional analysis of these issues but only a brief overview exposing the interplay of reasonableness, warrants, probable cause, and particularity in the context of electronic surveillance. For a more detailed discussion of these issues, I would again refer the Committee to the Levi and Kris testimony previously mentioned as well as to the discussion of the "calculus of reasonableness" that I set out in *Technology, Security and Privacy: The Fear of*

Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd, 7 Yale J. L. & Tech. 123; 9 Intl. J. Comm. L. & Pol'y 8 (Dec. 2004).

Warrantless Searches

The Constitutional prohibition on unreasonable searches is not accorded more weight than the permission to conduct reasonable searches — with or without a warrant.

In discussing the expansion of the scope of the Fourth Amendment to encompass non-trespassory electronic surveillance in Katz v. United States, 389 U.S. 347 (1967), Attorney General Levi in his 1975 testimony noted that the Supreme Court was focused not so much on what was physically done, but "on why it was done and what the consequences are likely to be." The central concern of the Fourth Amendment, he noted, was with intrusions to obtain evidence to incriminate the victim of the search. Therefore, in cases where other legitimate government interests — not primarily criminal prosecution of the subject — are served, the Court has repeatedly upheld warrantless searches, even without a showing of probable cause. Thus, for example, the Court has upheld warrantless administrative searches intended to protect the general welfare (for example, OSHA or EPA inspections), warrantless "special needs" searches (for example, drug testing in the work place or schools), and warrantless access searches (for example, at airports or court houses).

Likewise, in the case of foreign intelligence surveillance aimed at preventing terrorist attacks it can reasonably be argued that criminal prosecution is secondary to protecting national security or preventing terrorist attacks. Indeed, a footnote to the majority opinion in Katz, as well as Justice White's concurring opinion, left open the possibility that warrants may not be required for electronic surveillance undertaken for national security purposes. And, of course, United States v. United States District Court [Keith], 407 U.S. 297 (1972), although requiring warrants for domestic surveillance even in national security cases, suggests that foreign intelligence may not be subject to the same requirements. The point here is simply that any existing warrant requirement for foreign intelligence surveillance is a statutory constraint, not necessarily a Constitutional requirement.

Whether the Fourth Amendment requires a warrant in any case depends on the purpose and degree of intrusion and is intended to protect individuals from the consequences of the intrusion, particularly the use of evidence uncovered during the search for criminal prosecutions. Thus, another way to protect the same interests would be to limit the use of information gathered through warrantless surveillance. Indeed, Judge Posner has suggested that one way to minimize the impact on civil liberties of warrantless surveillance in counterterrorism applications would be to limit the use of "information gleaned by such surveillance for any purpose other than to protect national security." He argues that such a limitation would make more sense — and be more protective of civil liberties — than requiring pro forma warrants for electronic surveillance in this context.

Another area in which the Court has always upheld warrantless searches is at the border.

For example, in United States v. Ramsey the Court upheld the search without probable cause or a warrant of international first class mail as it entered the country. The Court observed that "border searches … have been considered 'reasonable' by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." The Court specifically rejected the argument that mail was somehow different and entitled to greater protection. Thus, it can reasonably be argued that interception of international communications — that is, communications that cross the border — are not subject to the warrant requirement even absent the more general foreign intelligence exception.

Probable Cause

The probable cause standard itself varies depending on the circumstances of the search. As Levi noted in his testimony, "In the *Keith* case, while holding that domestic national security surveillance, not involving activities of a foreign power and their agent, was subject to the warrant requirement, the Court noted that … a standard of probable cause to obtain a warrant different from the traditional standard could be justified: 'Different standards may be compatible with the fourth amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.'"

Indeed, FISA itself — enacted in part in response to *Keith* — provides a different probable cause standard than that required by Title III. Thus, in upholding the constitutionality of FISA against a Fourth Amendment challenge in United States v. Megahey, 553 F. Supp. 1180, 1188-89 (E.D.N.Y. 1982), the court held that although the foreign intelligence exception to the warrant requirement applies when surveillance is conducted for foreign intelligence purposes, the probable cause requirement itself is not "fixed or static" but depends on the circumstances. Thus, opined the court, a FISA warrant meets the probable cause standard of the Fourth Amendment even without the exception.

As Attorney General Levi stated: "although at one time the 'reasonableness' of a search may have been defined according to the traditional probable cause standard, the situation has now been reversed. Probable cause has come to depend on reasonableness — on the legitimate need of the Government and whether there is reason to believe that the precise intrusion sought, measured in terms of its effect on [the individual], is necessary to satisfy it."

Where there is a reasonable basis for believing that a communication has foreign intelligence value — that is, where there is a reasonable basis to conclude that one party to the communication is affiliated with al Qa'ida — limited electronic surveillance, even within the U.S. or where the other party is a U.S. citizen, is likely to meet the Constitutional probable cause standard (even if not the existing FISA standard). Indeed, as Attorney General Gonzales stated in January: "the standard applied [in the NSA

Terrorist Surveillance Program] — 'reasonable basis to believe' — is essentially the same as the traditional Fourth Amendment probable cause standard."

Particularity

The particularity requirement of the Fourth Amendment does not impose an irreducible requirement of individualized suspicion before a search can be found reasonable, or even to procure a warrant. In at least six cases, the Supreme Court has upheld the use of drug courier profiles as the basis to stop and subject individuals to further investigative actions. More relevant, the court in United States v. Lopez, 328 F. Supp 1077 (E.D.N.Y. 1971), upheld the validity of hijacker behavior profiling, opining that "in effect ... [the profiling] system itself ... acts as informer" serving as sufficient Constitutional basis for initiating further investigative actions.

And, Attorney General Levi specifically suggested in his testimony to the Church Committee that a different kind of warrant based on submitting programs of surveillance (designed to gather foreign intelligence information essential to the security of the nation but not based on individualized suspicion) for judicial review might be developed. Here he cited Justice Powell's opinion in Almeida-Sanchez v. United States, 413 U.S. 266 (1973), in which the possibility of using "area warrants" to obtain "advance judicial approval of the decision to conduct roving searches on a particular road or roads for a reasonable period of time" was suggested approvingly.

It should be noted that Levi went on to suggest that the development of any such new kind of extended warrant would require or benefit from a statutory base. However, he also suggested that in dealing with foreign intelligence surveillance "it may be mistaken to focus on the warrant requirement alone to the exclusion of other, possibly more realistic, protections."

Proposed Legislation

Finally, let me briefly comment specifically on three of the current legislative proposals that have circulated in draft form: the National Security Surveillance Act of 2006 (the "Specter bill"), the Terrorist Surveillance Act of 2006 (the "DeWine bill"), and the Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act (the "LISTEN Act"). Although I have read all three proposed bills closely and am familiar with many of the specific provisions — as well as with the detailed criticisms leveled against them by others, including other witnesses here today — I must confess that I'm not sure I understand all of the technical details of the Specter and DeWine bills. In any case, I do not intend to offer my own detailed comments here. Rather, I make three simple observations.

First, as already noted, I think the LISTEN Act addresses only the procedural deficiencies of the current FISA process rather than addressing its substantive failings. That said, I applaud the attempt to streamline and modernize the procedures for seeking and issuing

FISA warrants and would suggest that these provisions of the LISTEN Act be incorporated into any legislative solution addressing the substantive failings as well.

Second, the Specter bill attempts to address the substantive failings of FISA by authorizing the FISC to approve "electronic surveillance programs" designed "to gather foreign intelligence or protect against international terrorism or clandestine espionage activities" where it is not feasible to name every person or location to be subjected to electronic surveillance and where effective gathering may require an extended period of surveillance. The approach of the Specter bill to require judicial review by the FISC raises three fundamental questions:

1. Is the FISC constitutionally prohibited from fulfilling such a role by the case-or-controversy requirement under Article III? Kris in his testimony to the Senate Judiciary Committee cites a 1978 opinion of the Office of Legal Counsel to the Congress opining that FISA satisfied Article III and suggests that the reasoning set out in that opinion may have bearing on the programmatic review called for in the Specter bill.

2. Even if constitutionally permissible, is the FISC — or any court — ill-suited by experience or institutional temperament to review in the abstract an operational intelligence program, particularly where the potential effectiveness of the program is itself part of the criteria for judging its reasonableness? This is a more subjective question without a definitive answer. The FISC does have experience with issuing anticipatory warrants, and in reviewing and monitoring operational minimization procedures, and is generally familiar with intelligence program requirements. Additionally, the involvement of FISC may add to public confidence and acceptance of these programs, thus outweighing any potential negative concerns.

3. Is the judicial approval authorized by the Specter bill in the nature of a general warrant, and, therefore, constitutionally impermissible? Here I would again defer partially to Kris who suggests that the court order be considered not a "general warrant" but only an authorization for warrantless surveillance that is more likely to be reasonable under the Fourth Amendment because it is subject to advance judicial review. As already noted above, the Fourth Amendment allows for warrantless surveillance in certain circumstances. Alternatively, I would add my own view that a special warrant procedure, like that suggested by Attorney General Levi, authorizing specific "programs of surveillance" with a clear statutory basis would arguably survive a particularity challenge.

Third, the DeWine bill takes a similar approach as that in the Specter bill but would substitute intensive — but limited — legislative review of such surveillance programs for the judicial review called for in the Specter bill. In addition to the obvious questions regarding the appropriateness of Congressional versus judicial involvement in authorizing surveillance activity there is an additional concern raised by this approach: the DeWine bill would essential create a new class of intelligence activities subject to a novel oversight structure limiting operational oversight to small subcommittees of the

Intelligence Committees and divesting the Judiciary Committees of their jurisdiction. Thus, the DeWine bill not only amends FISA, but may undermine, or at least significantly amend, the oversight balance that currently exists under the National Security Act of 1947 requiring the administration to brief the full Intelligence Committees on all intelligence matters other than covert actions. It is unclear to me at this point that such a significant restructuring of intelligence oversight ought to be undertaken — or is necessary — simply to remedy the identified deficiencies in FISA. However, it is possible that there are additional operational or institutional concerns that I am not aware of that would justify this approach.

Before concluding I would again urge the Committee to review the recent testimony of David Kris before the Senate Judiciary Committee in which he not only offers his analysis of the Specter and DeWine bills but also offers his own draft legislation as a vehicle for a detailed discussing of many of the complex issues involved in this area. Although there are significant aspects of his analysis with which I disagree, on the whole I commend his "Comments on Possible Legislation" (the second part of his testimony) as extremely constructive to the debate.

Conclusion

In conclusion let me again thank the Committee for this opportunity to discuss foreign intelligence surveillance reform. As I stated at the beginning of my testimony, by all means let us debate who should authorize and oversight these surveillance programs but let us not forget that *someone* must and the existing mechanisms are inadequate. Thus, I commend the Chairman and this Committee for holding these hearings and for engaging in this endeavor.

Thank you and I welcome any questions that you may have.