A THE NEW REPUBLIC ONLINE DEBATE.
Tap Dancing

by Richard A. Posner & Philip B. Heymann

Post date: 01.31.06

Editor's Note:

In this week's edition of TNR, Judge Richard A. Posner defends President Bush's wiretapping program. Today, TNR Online presents day one of a weeklong debate between Posner and Harvard Law School Professor Philip B. Heymann.

Day 1: Tuesday, January 31

Dick, you argue that secret wiretapping forbidden by FISA may work, and if it does it may be desirable despite its costs, and if it's desirable it may be legal. It is muddling to fail to deal separately with these questions before merging them into one potpourri as you do. I am happy to discuss with you next time whether and on what conditions it would be a good balancing of counterterrorism and civil liberties to add listening to, or reading, Americans' overseas communications to the long list of less intrusive ways we have of looking for leads about citizens involved in terrorist plots. First we have to address what you call "aridly legal" in the present NSA scandal: the defiance of legislated prohibitions and the absence of published standards and any known system of accountability to the other branches.

I, like most Americans, don't want Americans detained by their president without legislated authorization that includes publicly announced standards and meaningful oversight. I don't want citizens of other countries interrogated without standards or rules that are announced and without real oversight. And no, I don't want my conversations listened into or my house searched without public standards and real accountability to insure that the standards are being complied with.

It happens that all these attitudes and beliefs have been made federal law. Congress and prior presidents have agreed with these beliefs and enacted statutes requiring the president to respect them. This president, the first to do so in my fifty years of political awareness, flatly claims a right to ignore any statute that he thinks stands in the way of unchecked powers to deal with terrorism. Your answer to all this is to say that concerns such as mine are "aridly legal" and relatively trivial matters compared to the immense advantages the country may gain in the form of intelligence.

There is just about everything wrong with your argument. It is naïve in confidently assuming a significant amount of rationality when the executive moves without legislated standards. The interrogations at Abu Ghraib are a powerful counterexample to this. So are the initial detentions of 1,000 aliens on immigration charges.

It is a huge mistake to think that any standards set publicly by legislation and any efforts at assuring some measure of accountability in complying with those standards are broadly inconsistent with the efficient pursuit of the counterterrorism objectives we may have in detaining, interrogating, and listening in on the phone calls of individuals. Monitoring communications is expensive in governmental resources as well as in citizen civil liberties. Intelligence as well as law enforcement agencies like to use far cheaper devices to develop leads and then allocate costly procedures where the evidence shows it is far more likely that they will find important information.

It is a mistake to think that it isn't a profoundly dangerous change in American executive power to accept a presidential claim to, secretly and without known standards, set aside statutes designed to protect American citizens against the clumsiness, wrong headedness, and occasional malice of executive officials.

You seem to want to debate whether it is possible or plausible that a properly created and publicly available standard for electronic surveillance might wisely authorize such surveillance with less than probable cause in order to patrol for terrorist plots. Senator DeWine proposed such an amendment to FISA only to have it rejected out of hand by the administration. But he forthrightly filled in the gaps. He openly defined coverage (non-U.S. persons) and standards (reasonable suspicion) and oversight (the FISA court). Instead you are defending a standardless, secret, unaccountable system of electronic surveillance that clearly violates a carefully considered statute. Should there have to be some reasonable suspicion? Should any such authorization apply only to oral communications or would it, like the FISA statute, apply to physical searches as well? Should the public be told the standards or would we have to guess? What system of accountability would let us know if my calls to my daughter who now lives in Montreal were subject to electronic surveillance as arbitrary and inane as interrogations at Abu Ghraib or detentions in the Brooklyn Detention Center? And should whatever secret system of the president's you are presently defending require an amendment to legislation that now very clearly prohibits it? Or do you accept the president's daunting claim to be free of any obligation to the law whenever he thinks that would be handy in fighting terrorism?

--Philip B. Heymann

Phil, I said I was not offering a legal opinion on the NSA surveillance program. I didn't think it would be appropriate for me to do so. What I argued was that so far as I can judge, the national security requires such a program, and the costs in liberty and privacy are acceptable and can be minimized by forbidding the use of the intercepted communications for anything other than the protection of national security, even if they contain evidence of other crimes.

You say that "First we have to address ... the defiance of legislated prohibitions and the absence of published standards and any known system of accountability to the other branches." Why *first*? The way I approach a case as a judge--maybe you think it heresy--is first to ask myself what would be a reasonable, sensible result, as a lay person would understand it, and then, having answered that question, to ask whether that result is blocked by clear constitutional or statutory text, governing precedent, or any other conventional limitation on judicial discretion. That is how I would proceed if asked to decide a case challenging the legality of the NSA surveillance program. I would try to find out as much as I could about the program--its contribution to national security and the inroads it makes on liberty and privacy--before I started waxing indignant over it, and that indeed is what I have tried to do, and the result of that inquiry is my article. I missed such an inquiry in the letter to Congress you co-signed that was published in *The New York Review of Books*.

If I am right that the NSA program probably contributes more to national security than it detracts from personal liberty, still it may be blocked, because not every good thing is legal. You and your co-signers have one view on that; the Department of Justice and Cass Sunstein (not a Republican shill) have another. I express no view. If the program is necessary for national security, then I am sure that it or some variant can be squared with law, if need be by amending FISA. I am curious whether you think FISA should be amended, and if so how.

Let me restate what I think the government needs to be able to do but FISA does not authorize it to do, and let me ask you whether you agree that the government needs to be able to do these things and, if so, what kind of controls you would suggest placing on such activity. According to the administration, the only communications intercepted outside the framework of FISA are calls to and from the United States in which the overseas party is suspected of terrorist connections, though the suspicion does not rise to the probable-cause level that would be required for obtaining a FISA warrant. It seems to me vital to our national security to be able to intercept such communications--and more. Suppose a phone number in the United States is discovered on a rolodex in an Al Qaeda hideout in Yemen. Wouldn't you want the NSA to intercept all calls, especially international, to or from that U.S. number and scrutinize them for

suspicious content? Yet the mere fact that a suspected or even a known terrorist has a U.S. phone number in his possession would not create probable cause to believe the owner of that phone also a terrorist; probably most phone conversations of terrorists are not with other terrorists. The government can't get a FISA warrant just to find out whether someone *is* a terrorist, though that's what it most needs to know. Nor can it obtain a warrant to intercept communications between two persons both of whom are in the United States, even if they are suspected of being members of a terrorist sleeper cell. These are crippling limitations.

I would have expected you to agree. For in your book *Terrorism and America: A Commonsense Strategy for a Democratic Society*, you identified "eight questions that are critical to prevention" of terrorism: "[1] Who are the members actively engaged in planning to use violence for political purposes? [2] What is their motivation? [3] Where are they located? [4] Who in the population is likely to join the group or provide forms of support needed for its continued operations? [5] What is the extent and nature of the support the group is receiving from others outside the country, including another state? [6] How does the group handle the problems of remaining clandestine and yet carrying out political violence? What is its *modus operandi*? [7] What type of attacks is the group capable of? [8] What is the strategy behind their planning?" These are questions to which electronic surveillance unfettered by the archaic limitations of FISA (a relic of the 1970s) might be expected to produce some answers.

Now you may think (do you?) the terrorist threat too slight, or the cost in privacy too great, to warrant such surveillance. I disagree on both counts. Regarding the second, I disagree with your apparent belief that physical and electronic searches are equally invasive of privacy. I would rather have my phone tapped by the NSA than have police conduct a search of my home. One effect of the digital revolution is that we've already surrendered most of our informational privacy to vendors, insurers, E-Z pass, etc., in exchange for modest economic benefits. I would be willing to surrender some of my remaining privacy to the NSA if that would reduce the risk of further terrorist attacks.

You define what you call "the present NSA scandal" as "the defiance of legislated prohibitions and the absence of published standards and any known system of accountability to the other branches [of government]." The government argues that FISA, because amended in effect by the 2001 Authorization for Use of Military Force, does not prohibit the program and that if it does it trenches on the President's Article II powers. The argument may be right or wrong, but if right--on which I take no position--there is no issue of "defiance." As for "published standards," they run the risk of tipping off the terrorists regarding forms of communication that the NSA may and may not intercept; secret programs have

their place in the struggle against global terrorism (do you agree?). As for "accountability to the other branches," let's await the outcome of the forthcoming Senate Judiciary Committee hearings and of the litigation challenging the program before concluding that the other branches have been reduced to helpless spectators.

UPDATE: In an effort to spare the reader the hideous details of the FISA statute, I remarked too cryptically and therefore misleadingly that the government cannot "obtain a warrant to intercept communications between two persons both of whom are in the United States, even if they are suspected of being members of a terrorist sleeper cell." I should have qualified the statement as follows: The government can obtain a warrant if it has not merely suspicion, but probable cause to believe, that the target is a member of a foreign terrorist gang. If the gang is domestic, however, then no warrant can issue even upon probable cause, because a FISA warrant is permissible only to obtain "foreign intelligence information." Finally, if the target is not a "U.S. person" (primarily meaning a U.S. citizen or lawful permanent resident), no warrant is required if the interception takes place outside the United States, but in the case of a domestic phone call, this will, I believe, rarely be possible.

--Richard A. Posner

Day 2: Thursday, February 2

Dick, it's worth laying out our areas of agreement before moving on to the areas where we disagree. I agree that statutory and constitutional interpretation of an ambiguous text can often be enlightened by a judgment as to what would be a sensible result in the situation and you agree that this isn't true when the document or precedent is unmistakably clear. I think the FISA statute unmistakably makes what the president has done illegal, unless the statute itself is unconstitutional. In your post, you cited a letter to Congress that I co-signed. For reasons laid out in a second letter to Congress that I co-signed, I think requiring the president to follow the law or get Congress to change it is plainly constitutional and, were it not, the country would be in one grand mess.

We seem to disagree as to where the discussion should begin. I suggested we first discuss the issue of legal authority and the equally important issues of having standards and accountability as a reminder of the immense social costs of what the president has done. To begin with the issue of whether FISA should be amended by Congress, as you proposed, would be to treat the issues before us as if they didn't involve all the consequences of a president secretly ignoring a statute limiting and defining executive powers, the implicit precedent for

searches of homes under an identical claim of constitutional authority, and all the risks of careless or intentional misuse of secret powers to invade communications that are thought to be private when there are no known standards and no outside review of what is done. I agree that now we should move on to your question: What if the president hadn't behaved in such a dangerous way but instead had forthrightly gone to Congress seeking an amendment of FISA? Would I oppose that?

Any answer to that question requires comparing the present law and the practice that surrounds it with the hypothetical presidential amendment. In particular, you often seem to be toying with the alternative of having any proposed new legislation impose no standard at all and no judicial oversight for targeting the content of international communications of U.S. persons. Only that might maximize the prospects of detecting information about a plot within the United States or, also valuable, discouraging communications between terrorists and U.S. supporters. Let's begin with that as the alternative to FISA as it is today.

Note that we are setting aside a set of interesting questions. First, we are not considering the quite separate issue of obtaining the "envelope"-type information about phone calls or e-mail that simply tells the NSA to whom a message is going or from whom it came. These matters get no constitutional protection in the United States and very little statutory protection. We are also setting aside for now the Defense Department's capacity to analyze this and other data in richly imaginative ways--a form of data-mining that is in no way prohibited either by the Constitution or by statute. Finally, although the issues are messier, as well as more interesting, we are delaying for now any questions about using a Google-like search engine on masses of communications looking for content that would itself create and justify suspicions of terrorism. Our subject is simply targeting the communications of Americans in the United States for their content.

How can we assess the trade-offs in terms of both national security and civil liberties between your proposal and present law? Would the advantage of dispensing with the requirement of probable cause or even "reasonable suspicion" help to fight terrorism enough to offset the costs in terms of reduced privacy and a sense of security in one's conversations?

To be clear in considering the present FISA rules we have to include the practices that surround them. The way the system works we rely on something other than listening to the phone calls of Americans both to raise the initial suspicions of (i.e., to detect) terrorist planning and to carry out a second stage where the suspicions lead to further investigative steps that can themselves warrant arrest, search, or electronic surveillance. You seem somewhat preoccupied with the idea that the government can't engage in any one of these latter activities, which

require probable cause, as a way to detect suspects or even to begin to build suspicions to an adequate probability. That has not proved to be a great problem.

There are probably a dozen ways at least as promising as listening in to phone calls without probable cause that we use to detect terrorist plots and build toward probable cause. The government can target the foreign end of any phone conversation of non-Americans. It can get additional suspects by listening in, with probable cause, even when (you seem mistaken here) both parties are Americans within the United States. It can freely pick up the "envelope" information as to who is communicating with whom abroad and, without anything like probable cause, within the United States. It can use data-mining of this information and available commercial information to apply templates which themselves reveal terrorists. It can send agents to attend any meeting where individuals are likely to be recruited. Several of these steps may, when combined, amount to probable cause for an arrest, a search, or electronic surveillance. So can a tip from a source. To move from suspicion to probable cause, the government can also use paid or unpaid informants, physical surveillance, and undercover offers. I suspect I'm missing a variety of other steps.

This is the background of a quite rich array of alternatives to accomplish the initial detection and the second stage of building on detection, which you correctly identify as critical. The question that divides us, stated precisely, is whether the benefits of adding to this array a capacity to listen in to international phone conversations of Americans within the United States without either probable cause or reasonable suspicion (we would have to discuss that standard separately) adds more in the way of detection against terrorism than it costs in terms of civil liberties. What it adds is an additional form of detection that would also bypass the second stage of building probable cause. It would thus add marginally to the number of cases where such a search took place usefully, because sometimes the government can't take the steps from detection to probable cause even though the suspect may be a dangerous plotter. On the other hand, the American plotter would have to be particularly foolish to be communicating about terrorist plans in so obvious a way with those he or she knows we could have identified as terrorists abroad. Still, all told, there would be some marginal gain.

What would the costs of the change be, assuming that the president forthrightly went to Congress to seek it and thus eliminated much of the threat to our separation of powers? There would be a very substantial inhibition of intimate communications. I would discuss family members far more carefully with my daughter in Montreal. There would be a reduction in political debate, particularly critical of the government, over whatever communication channels were subject to patrol. As the FBI complains, the expenditure of investigative

time would be immense with the resulting opportunity cost of being able to use less of one of the other detection devices that are harder for a terrorist plotter to avoid. There would be an inevitable shift of power to the executive branch simply on the theory that knowledge is power, and a shift within the executive branch to the Department of Defense, and within the Department of Defense to those having access to the "take." There would be a plausible precedent for physical searches of the sort you object to much more.

So, if I have been careful and precise in describing the trade-offs, I think we are looking at marginal possible gains in intelligence and very real and certain costs in civil liberties. One final point: Of course, we have to multiply even a tiny reduction in risk by the size of the danger, which in the case of a nuclear bomb is immense. (You are mistaken in thinking that a "dirty bomb" is even remotely comparable in its dangers.) But we cannot allow that threat to justify every imaginable step that reduces its probability even slightly. If we did we would live in a state of huddled fear for the next 30 or 40 or 100 years. There are far better ways to reduce the threat of nuclear terrorism.

Finally, published standards for an investigative step do not necessarily provide any useful information to terrorists. Standards like probable cause or even reasonable suspicion provide practically no information to a terrorist who never knows where the government's information lies between enough suspicion to expend the resources to listen to his or her communications and the ability to meet one of those standards.

--Philip B. Heymann

Phil, you say that I'm "mistaken in thinking that a 'dirty bomb' is even remotely comparable in its dangers" to a nuclear bomb. But according to Senate testimony given in 2002 by a representative of the Federation of American Scientists concerning dirty bombs, "Materials that could easily be lost or stolen from U.S. research institutions and commercial sites could contaminate tens of city blocks at a level that would require prompt evacuation and create terror in large communities even if radiation casualties were low. Areas as large as tens of square miles could be contaminated at levels that exceed recommended civilian exposure limits. Since there are often no effective ways to decontaminate buildings that have been exposed at these levels, demolition may be the only practical solution. *If such an event were to take place in a city like New York, it would result in losses of potentially trillions of dollars* [emphasis added]."

This is a minor point, but illustrative. I think you underestimate the danger of terrorism. And I think you're mistaken in what you think FISA allows (I wish you were right!) and in your preference for alternatives to electronic surveillance

that might well do greater damage to liberty and privacy.

You say that if all that the NSA learns from a phone call or e-mail is "to whom a message is going or from whom it came" it receives "very little statutory protection." Actually, as I read FISA, the receiver's name gets the same protection as any other part of the contents of an intercepted communication. The Act defines electronic surveillance as acquiring "the contents" of an electronic communication and defines "contents" to include "any information concerning the identity of the parties" or indeed the "existence" of the communication.

You further suggest that "data-mining" presents no legal problems, nor "using a Google-like search engine on masses of communications looking for content that would itself create and justify suspicions of terrorism." It is true that a computer search is not a search within the meaning of the Fourth Amendment or a form of electronic surveillance within the meaning of FISA. But if the search flags a communication as suspicious the (human) intelligence officer cannot read it or otherwise acquire its "substance, purport, or meaning" (additional terms in the statutory definition of "contents") without a warrant, that is, without probable cause.

You say "the government can target the foreign end of any phone conversation of non-Americans." Not so; a warrant is required if one of the foreigners is in the United States and the interception occurs here. You say correctly that the government can listen in, "with probable cause, even when ... both parties are Americans within the United States." But it must be probable cause to believe that the target is engaged in *international* terrorism. And probable cause is too high a standard when the goal is to discover who *is* a terrorist, as you acknowledge in stating that only methods *other than* electronic surveillance may be used "to raise the initial suspicions of (i.e., to detect) terrorist planning." You ask whether dispensing with "reasonable suspicion" would advance the struggle against terrorism, but FISA does not permit searches based on reasonable suspicion and you don't want to amend FISA.

You were a high Justice Department official in the 1990s and maybe the interpretations of FISA in your post reflect a certain looseness in how the Department interpreted the law. I would not object strenuously!

You say that the government "can send agents to attend any meeting where individuals are likely to be recruited. ... To move from suspicion to probable cause, the government can also use paid or unpaid informants, physical surveillance, and undercover officers." This is true but incomplete. The government need not have even bare suspicion to do any of these things, because they are not classified as searches. I do not understand how liberty and privacy

are secured by deflecting the intelligence services from electronic surveillance to the intelligence methods you list. The FBI can if it wants send intelligence officers into mosques, masquerading as members of the congregation. It can bribe the real members to spy for it and to report what the imam says and how the congregation responds. It can collect from public sources information about the imam and the enthusiasts in his congregation or even follow the imam and the enthusiasts around and photograph or eavesdrop on them. The Bureau will do more of these things the fewer electronic-surveillance leads it receives from the NSA and has to follow up. Would you regard that as a gain for civil liberties?

And speaking of civil liberties, and at the risk of seeming even more insensitive than I am, I do not understand your worry about discussing family members with your daughter in Montreal, which you have now brought up twice. I don't know your family, but it strikes me as unlikely that an NSA search program would flag such a discussion as suspicious and thus trigger an intelligence officer's listening to your conversations. Do you think that if your daughter tells you that her aunt is the family bore, the NSA or the FBI is going to open a file on the aunt?

I said in my initial post that I didn't want to offer a legal opinion on the NSA program, and I don't; but I also don't want to let pass the hyperbole (as it seems to me) in the beginning of your post. You say that "the FISA statute unmistakably makes what the president has done illegal, unless the statute itself is unconstitutional," and you are certain that it is not. As Cass Sunstein has argued, if there is any significant doubt about the statute's constitutionality, that is a reason for interpreting the Act as not outlawing the NSA program. The Act does not forbid electronic surveillance outside the framework of the Act itself if it is authorized by another statute, and the argument of course is that the Authorization for Use of Military Force--Congress's September 14, 2001 "declaration of war" against Al Qaeda--is such a statute. Nor is the constitutional argument frivolous. It is that once we are at war, the president's inherent wartime authority as commander in chief clicks in and encompasses signals intelligence. I'm sure you agree that Congress could not have passed a law in 1944 ordering the president to move D-Day to July 4.

In listing these arguments for the legality of the NSA program, I do not mean to endorse them. I do not myself consider Al Qaeda-style terrorism to fit neatly into either the box we label "crime" or the box we label "war." I think it's sui generis and should be treated accordingly. I also don't know where exactly the line falls between the president's prerogative authority to control military operations and the provision in Article I of the Constitution that authorizes Congress to "make Rules for the Regulation and Government" of the armed forces. I object merely to your oversimplifying the legal issues. The oversimplification, and the

indignation that it engenders, exacerbate political divisions, of which we have enough already.

--Richard A. Posner

Day 3: Sunday, February 5

Dick, I hate taking up too much of our space—that should be used to carry on the debate the President has so carefully avoided—sparring with you about matters that don't affect the heart of our arguments. I have tried very hard not to engage in "oversimplifying the legal issues," although I am in fact indignant at the efforts of the administration to prevent the type of discussion that would reveal the issues in their complexity and nuance. That's what I've been trying to do. I think you are too, even though I believe you're continuing to make legal and factual mistakes (of no great consequence).

When a phone call is to or from a place abroad, the NSA can target it without any reference to the FISA court, unless it knows it's dealing with a U.S. person. The same is of course true of picking up phone numbers of calls, or electronic messages, to or from a non-U.S. person abroad. FISA is simply not an extra-territorial statute. The Supreme Court's Verdugo case holds as much as to the Constitution.

If the government wants to get the numbers or email addresses of people calling to or from a person it suspects in the United States, perhaps because it has picked up a call to him from a non-U.S. person abroad, it is the job of the FBI to seek permission under 50 USC 1842, which requires no more than "a certification by the applicant…that the information likely to be obtained…is relevant to an ongoing investigation to protect against international terrorism…." Nothing in the FISA statute forbids the NSA from being the applicant, but we have a strong tradition of keeping the military out of domestic arrest, searches, and electronic surveillance, except to protect military installations. You are right of course that the definition of contents includes "any information concerning the identity of the parties," but that definition doesn't affect the legality of the pen register, trap-and-trace device, or of any other form of electronic surveillance.

If the NSA is either targeting non-U.S. persons abroad or engaged in a Google-like search of foreign communications, it can discover and retain any information that is relevant to terrorism even if it involves U.S. persons and even if the other party to the conversation is a U.S. person in the United States. No warrant or probable cause is necessary. None of this is very surprising, the NSA has operated effectively for twenty years against the agents, domestic or foreign, of a

superpower with tens of thousands of nuclear warheads, some of suitcase size, and a difficult-to-detect network of terrorist surrogates.

As to the relatively minor dangers of a "dirty bomb" compared to a nuclear bomb, I suggest you read what the U.S. Nuclear Regulatory Commission has to say (http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs.html):

At the levels created by most probable sources, not enough radiation would be present in a dirty bomb to kill people or cause severe illness.

The Commission notes that a major danger may well be unreasonable panic and advises that "accurate, non-emotional public information might prevent the panic sought by terrorists."

Dick, let's get back on track. Even if you were right about our factual and legal disputes, this would not change the core of our debate. Nor are our positions on civil liberties and national security far apart, although I am outraged by the President's secret program. In ***Protecting Liberty in an Age of Terror***, Juliette Kayyem and I called for legislation to expand in carefully defined ways the authority of NSA while still giving much the same respect to the privacy of communications of U.S. persons within the United States as law enforcement is required to give. We even reserved the possibility of greater NSA powers in situations of clear and immediate danger of attack—a reservation very close to the present exemption of NSA for 15 days after the beginning of a war. With all of that out of the way, can we now turn to the heart of our disagreement?

You began by posing a conflict between "arid" law and the necessities of national security. But considerations of judicial propriety kept you from stating a view on two crucial questions: how clearly did the FISA statute forbid the President's wiretapping program and, if it clearly did, how persuasive was the argument that the President's wartime powers made unconstitutional any application of the statute that would forbid that program? I responded by insisting that we give great weight to democratic processes in addition to national security. I emphasized the dangers of any president acting secretly to set up a program of electronic surveillance of Americans in America, without announced standards, without any review outside the executive branch, and especially, but not only, in defiance of a federal statute.

You pressed for my views on whether a statute giving the President the powers he has secretly taken would be desirable. I argued that it would not, at least if the President continued to act without known standards and any outside accountability. The gains from that type of electronic surveillance of Americans

are not, on careful analysis, very great compared to the presently available tools of detection. To assess benefits one must consider all the other ways of detecting terrorists and especially those terrorists who are too intelligent to speak openly with known terrorists abroad about their terrorist plots. The losses in democratic values and the rule of law, on the other hand, are very great.

Here are my bottom line arguments and conclusions:

1) The issue of trade-offs between national security and civil liberties in amending the FISA statute would richly deserve legislative hearings and a careful legislative resolution, if there were to be any startling change. There is something terribly harmful for a democracy about having the President resolve these issues secretly and, in the course of that, ignore or defy a clear federal statute.

2) Whoever proposes a substitute statute should bear a very heavy burden of persuasion unless that substitute includes both a statement of the standards under which Americans could be subjected to electronic surveillance at home and an adequate system of oversight to guarantee that those standards were met. Moreover, any changed standard would, like the DeWine proposals, have to specify to whom it applied, to what communications, and in what situations (for example, of urgent danger). Writing law is about drawing lines. Without these, there is dangerous power without law. Such power was misused by Nixon and Kissinger. A closely related power was misused by someone to go after U.S. Ambassador Joseph Wilson. U.N. Ambassador John Bolton may or may not have had an innocent explanation for wanting to read what NSA was picking up about Americans.

3) Your image of a sleeper cell with nuclear weapons that will be activated only on receiving a readable international communication from a known terrorist abroad seems to me unlikely and, in any event, far too sweeping in the implications you would draw from it. The benefit of monitoring whatever international communications the President decides should be listened to depend upon how much it adds to the array of devices already in place. It also depends upon the other ways such a terrible event could be prevented, such as locking down fissile materials and nuclear weapons and on what we do to also reduce the availability of safer ways for terrorists to communicate. You argue that denying the right to listen in on American's communications, at least international ones, will result in worse invasions of privacy (under the techniques I've described as plainly permissible). But there is absolutely no evidence, and very little likelihood, that either the FBI or the President would compensate for a rejection of the President's secret wiretap program by flooding

mosques with agents. Even if we thought that would happen, I would want the Congress to decide—not the President secretly—which was the preferable tool.

4) Many of these issues should be decided in court. Only the administration's most vigorous and imaginative efforts have kept these issues away from the courts—a set of efforts whose purpose is revealing of serious administration doubts about legality.

In short, this is no way to run a railroad—behaving secretly, creating suspicion, ignoring statutes, avoiding analysis, preempting debate, and keeping legal issues away from the courts. That adds up to a rather shabby operation.

--Phil Heymann

Phil, I'll follow the sequence of your discussion, and thus start with the retail factual and legal issues. Readers bored with such details can skip to Part II--and readers bored with the debate can skip to Part IV, where I offer constructive suggestions for "domesticating" post-FISA electronic surveillance.

I. If FISA is as loose as you suggest, this lowers the stakes in the debate--for you as well as for me, for it reduces the *incremental* effect of the NSA surveillance program on privacy. But I don't think it's that loose. The statute defines "electronic surveillance" to include "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." A "person in the United States" is not a "U.S. person," defined (primarily) as either a citizen or a lawful permanent resident. It's only when all parties to the communication are abroad, or the target is not a U.S. person and the interception occurs outside the United States, that no warrant is required for the interception.

The problem (turning now to your third paragraph) is not getting the phone numbers of the person the government suspects, but intercepting calls to and from those numbers without probable cause to believe that the suspect really is a terrorist. You don't want to amend FISA to lower the standard from probable cause to reasonable suspicion or bare suspicion. I repeat my example from my first post: If a U.S. phone number is discovered in an Al Qaeda hideout in Yemen, I want the NSA to intercept all calls, especially international, to or from that U.S. number and scrutinize them for suspicious content. Yet the mere fact that a suspected or even a known terrorist has a U.S. phone number in his possession would not create probable cause to believe the owner of that phone also a terrorist.

You're correct that if a lawfully intercepted communication reveals information about people in the United States, that information is not off limits. The problem comes at the next stage--establishing probable cause to intercept their communications. What you must be envisaging in such a case is the FBI sending agents to follow the individual around, obtain open-source materials on him, etc., in an effort to obtain probable cause to wiretap him. How such activities respect privacy eludes me. Would you rather be followed by FBI agents or be subject to NSA interception of your phone conversations with your daughter? And of course no purely domestic communications can be intercepted, with or without a warrant, except in accordance with Title III.

I said I thought you underestimated the terrorist threat, and I find further confirmation in your quotation from the Nuclear Regulatory Commission that "at the levels created by most *probable* sources, not enough radiation would be present in a dirty bomb to kill people or cause severe illness [emphasis added]." We cannot worry just about the "probable" forms of terrorist attack. Suppose the probability of a terrorist attack on a subway that would kill 30 people is 5 percent over some interval, and the probability of a nuclear attack is only 1 percent. In deciding how to configure our intelligence system, should we be thinking only about the higher-probability attack? That wouldn't be sensible cost-benefit analysis.

II. I understood you to be saying in your second post that you did not want FISA to be amended. But now you express support for enlarging the National Security Agency's authority--surely that would mean amending FISA. You state that your book with Juliette Kayyem recommends such enlargement. I do not doubt it, but I cannot find it, as there is no index reference to the NSA.
You mention FISA's 15-day rule. This to me is a clear example of an unconstitutional provision; and when I cautioned against "oversimplifying legal issues," one of the things I was thinking of was the failure of the signatories to the letters to Congress protesting the NSA program, co-signed by you, to engage with the serious issues of constitutionality that FISA, or at least some provisions of it, present. FISA allows the president to conduct warrantless electronic surveillance for up to 15 days after a declaration of war by Congress. Suppose the United States is invaded and it takes several days to convene Congress; during that interval, is the president barred from conducting warrantless electronic surveillance? I think not; the FISA bar trenches on the president's authority conferred by Article II of the Constitution to command the armed forces. The broader argument is that the Authorization for Use of Military Force is a declaration of war, and that once war is declared the president's Article II authority clicks in, regardless of what Congress foresaw, and that authority includes the authority to conduct signals intelligence. I do not say the argument

is correct; but is it weaker than arguments that have repeatedly carried the day in the Supreme Court? If not, why the indignation?

III. You summarize your position in four conclusions, and let me restate and comment on them briefly:

1. *It was "terribly harmful for democracy" for the president to change the ground rules for electronic surveillance without legislation and in the course of that change "ignore or defy a clear federal statute."* FISA is not clear, and if it doesn't block what the President did, he had no obligation to await legislative authorization.

2. *Any amendment to FISA should contain both clear statement of standards and an adequate system of oversight.* I don't disagree; I return to this point in Part IV.

3. *The benefits of expanded electronic surveillance should be evaluated in incremental terms, by asking what it adds to the existing array of preventive and reparative measures for dealing with terrorist attacks.* I agree. *It is highly unlikely that either the FBI or the president would compensate for a rejection of the President's secret wiretap program by flooding mosques with agents.* "Flooding"--no. But electronic surveillance and other methods of intelligence are substitutes--that is your point. If you have two substitute goods, and one is withdrawn from the market, demand for the other will increase.

4. *Many of these issues should be decided in court.* FISA creates civil and criminal penalties, though not for violating FISA--for electronic surveillance not authorized by statute. The statute doesn't have to be FISA; it could conceivably be the AUMF. There are several civil lawsuits pending challenging the NSA program. I do not know whether the plaintiffs can overcome standing problems (were *their* communications intercepted?); if not, there may be no mechanism for obtaining judicial review of the program. But I take no position on that question.

IV. I want to end on a constructive note. I think your real concern--or perhaps it is what I think your real concern should be--is with a return to the regime of electronic surveillance for national security that existed before 1978, when FISA was enacted, and especially before 1972, when the *Keith* case was decided. In that era, there were no standards, and there was no oversight, and I can understand how, especially with advances in communications technology, such a void would be particularly troublesome today. So let's try to fill it.

But not by constraining the president to comply with FISA as currently drafted. The statute, enacted long before the terrorist menace assumed its current shape and terrorism employing weapons of mass destruction became a serious concern, is thoroughly obsolete. The government should in my opinion be authorized to

intercept any electronic communication that contains information relating to national security, but should be forbidden to use that information for any purpose other than national security. The NSA would thus be forbidden to turn over any intercepted communication to the Justice Department for possible prosecution of a party to the communication for any offense other than a violation of a criminal law specifically designed for the protection of national security. This control measure would go far to alleviate privacy concerns aroused by electronic surveillance.

Furthermore, electronic surveillance beyond the bounds of FISA should be strictly limited to the collection of information relating to activities that threaten to cause *major* loss of life, or comparable harm to the public welfare. In other words, "national security" should be defined narrowly and "defining terrorism down" avoided. "Terrorism" could be defined as any political crime inflicting or threatening personal injury or property damage, thus including "eco[logical]terrorism" and attacks on laboratories by animal-rights nuts. I would confine electronic surveillance (outside its use in ordinary criminal investigations governed by Title III) to terrorist threats grave enough to count as real menaces to national security.

More in the way of control over a broad program of national security electronic surveillance is possible. But I do not think that a warrant requirement would be an effective method of control; nor should the delay and paperwork burdens of such a requirement be underestimated. Warrants are intended for situations in which we do not want the police to do something (like search one's home) without particularized grounds for believing that there is illegal activity going on. (That is true of physical searches, which FISA also authorizes; and there the warrant requirement should be retained.) All that the application for a warrant to conduct the kind of surveillance that I have described could say is that there is reason to believe that the surveillance might yield clues to terrorist identies, plans, or connections. That's not much of a filter, especially when we bear in mind that the FISA court is composed of judges appointed by the Chief Justice of the United States without Senate confirmation, judges willing to undergo the background investigation required for a top-secret security clearance and therefore presumably sympathetic to claims of national security, judges hearing only the government's side of the case because warrant proceedings are ex parte, judges asked to issue a warrant to protect the nation against potential dangers far greater than that of ordinary crimes for which search warrants are sought. In these circumstances, the danger is that the warrant primarily--and perversely--serves its historical function of shielding government officers from damages suits, since unless a warrant is procured fraudulently the officers who execute it will normally be shielded from civil liability.

We rightly worry when governmental power is concentrated, but a partial offset is that when power is concentrated so is responsibility. It may be better for the president to assume the full responsibility for conducting electronic surveillance intended to detect rather than to prove, rather than attempt to diffuse responsibility by enlisting the participation of judges under conditions in which they would be unable to exercise an effective check on executive power. We are not well served by judicial fig leaves.

The executive branch contains many regulatory structures to channel and check the discretionary activities of civil servants, including national security personnel. These can be adapted to regularize the broader electronic-surveillance authority that I believe the president should have, when the surveillance targets U.S. citizens and lawful permanent residents. Here are some possible measures to consider:

1. The Intelligence Reform and Terrorism Prevention Act of 2004 created the position of Civil Liberties Protection Officer in the Office of the Director of National Intelligence, and also a Privacy and Civil Liberties Oversight Board in the Executive Office of the President. These entities could be given special responsibility for monitoring electronic surveillance.

2. The National Security Agency could be removed from the Defense Department and placed under civilian control. This is independently desirable for reasons discussed in my forthcoming book *Uncertain Shield*. (Of course, it isn't going to happen!)

3. An electronic surveillance oversight board composed primarily of lawyers with civil-liberties expertise could be created to perform additional monitoring.

4. A steering committee for electronic surveillance could be created composed of the attorney general, the Director of National Intelligence, the Secretary of Homeland Security, and perhaps a senior retired judge or justice appointed by the Chief Justice of the United States.

5. Administrative controls could be instituted similar to those that Canada has placed on the Canadian Security Intelligence Service, which is the Canadian agency responsible for domestic intelligence.

6. The Director of National Intelligence could appoint a Director of Domestic Intelligence, who would have broad supervisory authority over all intelligence directed at U.S. citizens and lawful permanent residents.

Finally, regarding legislative oversight, although Congress has a good record of not leaking classified information, there is a natural sensitivity in the executive branch to sharing highly sensitive intelligence information too widely. A solution might be to appoint a very small joint House-Senate committee to oversee electronic surveillance, all members and staff of which would be cleared for access to top-secret materials.

These are just suggestions, intended to illustrate that "domesticating" sensitive intelligence activities does not require secret courts and obsolete statutes.

--Richard A. Posner

Richard A. Posner is a federal circuit judge and the author of the forthcoming *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform*.

Philip B. Heymann is former U.S. deputy attorney general, coauthor with Juliette Kayyem of *Protecting Liberty in an Age of Terror*, and Professor at Harvard Law School.