

**From:** b(3) - 50 USC 3024(m)(1)  
**To:** <Steve.Bradbury@usdoj.gov>, <rachel.brand@usdoj.gov>, <Kyle.Sampson@usdoj.gov>, "Allen, Michael", "Erin Joshi", P6/b(6), b(3) - 50 USC 3024(m)(1)  
b(3) - 50 USC 3024(m)(1), "Kelley, William K.", "Addington, David S.", "Yanes, Raul F.", b(3) - 50 USC 3024(m)(1)  
"Kavanaugh, Brett M.", "Coffin, Shannen W.", "Perino, Dana M."  
**Subject:** Posner  
**Received(Date):** Thu, 26 Jan 2006 14:24:54 -0500

fyi.



Searching for the perfect mix.



## THE NEWREPUBLIC ONLINE

WHAT IF WIRETAPPING WORKS?

### Wire Trap

by Richard A. Posner

Post date: 01.26.06

Issue date: 02.06.06

**T**he revelation by *The New York Times* that the National Security Agency (NSA) is conducting a secret program of electronic surveillance outside the framework of the Foreign Intelligence Surveillance Act (fisa) has sparked a hot debate in the press and in the blogosphere. But there is something odd about the debate: It is aridly legal. Civil libertarians contend that the program is illegal, even unconstitutional; some want President Bush impeached for breaking the law. The administration and its defenders have responded that the program is perfectly legal; if it does violate fisa (the administration denies that it does), then, to that extent, the law is unconstitutional. This legal debate is complex, even esoteric. But, apart from a handful of not very impressive anecdotes (did the NSA program really prevent the Brooklyn Bridge from being destroyed by *blowtorches*?), there has been little discussion of the program's concrete value as a counterterrorism measure or of the inroads it has or has not made on liberty or privacy.

Not only are these questions more important to most people than the legal questions; they are fundamental to those questions. Lawyers who are busily debating legality without first trying to assess the consequences of the program have put the cart before the horse. Law in the United States is not a Platonic abstraction but a flexible tool of social policy. In analyzing all but the simplest legal questions, one is well advised to begin by asking what social policies are at stake. Suppose the NSA program is vital to the nation's defense, and its impingements on civil liberties are slight. That would not prove the program's legality, because not every good thing is legal; law and policy are not perfectly aligned. But a conviction that the program had great merit would



shape and hone the legal inquiry. We would search harder for grounds to affirm its legality, and, if our search were to fail, at least we would know how to change the law--or how to change the program to make it comply with the law--without destroying its effectiveness. Similarly, if the program's contribution to national security were negligible--as we learn, also from the *Times*, that some FBI personnel are indiscreetly whispering--and it is undermining our civil liberties, this would push the legal analysis in the opposite direction.

Ronald Dworkin, the distinguished legal philosopher and constitutional theorist, wrote in *The New York Review of Books* in the aftermath of the September 11 attacks that "we cannot allow our Constitution and our shared sense of decency to become a suicide pact." He would doubtless have said the same thing about *fisa*. If you approach legal issues in that spirit rather than in the spirit of *ruat caelum fiat iusticia* (let the heavens fall so long as justice is done), you will want to know how close to suicide a particular legal interpretation will bring you before you decide whether to embrace it. The legal critics of the surveillance program have not done this, and the defenders have for the most part been content to play on the critics' turf.

**W**ashington, D.C., which happens to be the home of *The New Republic*, could be destroyed by an atomic bomb the size of a suitcase. Portions of the city could be rendered uninhabitable, perhaps for decades, merely by the explosion of a conventional bomb that had been coated with radioactivematerial. The smallpox virus--bioengineered to make it even more toxic and the vaccine against it ineffectual, then aerosolized and sprayed in a major airport--could kill millions of people. Our terrorist enemies have the will to do such things. They may soon have the means as well. Access to weapons of mass destruction is becoming ever easier. With the September 11 attacks now more than four years in the past, forgetfulness and complacency are the order of the day. Are we safer today, or do we just feel safer? The terrorist leaders, scattered by our invasion of Afghanistan and by our stepped-up efforts at counterterrorism (including the NSA program), may even now be regrouping and preparing an attack that will produce destruction on a scale to dwarf September 11. Osama bin Laden's latest audiotape claims that Al Qaeda is planning new attacks on the United States.

The next terrorist attack (if there is one) will likely be mounted, as the last one was, from within the United States but orchestrated by leaders safely ensconced abroad. So suppose the NSA learns the phone number of a suspected terrorist in a foreign country. If the NSA just wants to listen to his calls to others abroad, *fisa* doesn't require a warrant. But it does if either (a) one party to the call is in the United States and the interception takes place here or (b) the party on the U.S. side of the conversation is a "U.S. person"--primarily either a citizen or a permanent resident. If both parties are in the United States, *no* warrant can be issued; interception is prohibited. The problem with *fisa* is that, in order to get a warrant, the government must have grounds to believe the "U.S. person" it wishes to monitor is a foreign spy or a terrorist. Even if a person is here on a student or tourist visa, or on no visa, the government can't get a warrant to find out whether he is a terrorist; it must already have a reason to believe he is one.

As far as an outsider can tell, the NSA program is designed to fill these gaps by conducting



warrantless interceptions of communications in which one party is in the United States (whether or not he is a "U.S. person") and the other party is abroad and suspected of being a terrorist. But there may be more to the program. Once a phone number in the United States was discovered to have been called by a terrorist suspect abroad, the NSA would probably want to conduct a computer search of all international calls to and from that local number for suspicious patterns or content. A computer search does not invade privacy or violate *fisa*, because a computer program is not a sentient being. But, if the program picked out a conversation that seemed likely to have intelligence value and an intelligence officer wanted to scrutinize it, he would come up against *fisa*'s limitations. One can imagine an even broader surveillance program, in which *all* electronic communications were scanned by computers for suspicious messages that would then be scrutinized by an intelligence officer, but, again, he would be operating outside the framework created by *fisa*.

The benefits of such programs are easy to see. At worst, they might cause terrorists to abandon or greatly curtail their use of telephone, e-mail, and other means of communicating electronically with people in the United States. That would be a boon to us, because it is far more difficult for terrorist leaders to orchestrate an attack when communicating by courier. At best, our enemies might continue communicating electronically in the mistaken belief that, through use of code words or electronic encryption, they could thwart the NSA.

So the problem with *fisa* is that the surveillance it authorizes is unusable to discover who is a terrorist, as distinct from eavesdropping on known terrorists--yet the former is the more urgent task. Even to conduct *fisa*-compliant surveillance of non-U.S. persons, you have to know beforehand whether they are agents of a terrorist group, when what you really want to know is who those agents are.

*Fisa*'s limitations are borrowed from law enforcement. When crimes are committed, there are usually suspects, and electronic surveillance can be used to nail them. In counterterrorist intelligence, you don't know whom to suspect--you need surveillance to find out. The recent leaks from within the FBI, expressing skepticism about the NSA program, reflect the FBI's continuing inability to internalize intelligence values. Criminal investigations are narrowly focused and usually fruitful. Intelligence is a search for the needle in the haystack. FBI agents don't like being asked to chase down clues gleaned from the NSA's interceptions, because 99 out of 100 (maybe even a higher percentage) turn out to lead nowhere. The agents think there are better uses of their time. Maybe so. But maybe we simply don't have enough intelligence officers working on domestic threats.

**I** have no way of knowing how successful the NSA program has been or will be, though, in general, intelligence successes are underreported, while intelligence failures are fully reported. What seems clear is that *fisa* does not provide an adequate framework for counterterrorist intelligence. The statute was enacted in 1978, when apocalyptic terrorists scrambling to obtain weapons of mass destruction were not on the horizon. From a national security standpoint, the statute might as well have been enacted in 1878 to regulate the interception of telegrams. In the



words of General Michael Hayden, director of NSA on September 11 and now the principal deputy director of national intelligence, the NSA program is designed to "detect and prevent," whereas "fisa was built for long-term coverage against known agents of an enemy power."

In the immediate aftermath of the September 11 attacks, Hayden, on his own initiative, expanded electronic surveillance by NSA without seeking fisa warrants. The United States had been invaded. There was fear of follow-up attacks by terrorists who might already be in the country. Hayden's initiative was within his military authority. But, if a provision of fisa that allows electronic surveillance without a warrant for up to 15 days following a declaration of war is taken literally (and I am not opining on whether it should or shouldn't be; I am not offering any legal opinions), Hayden was supposed to wait at least until September 14 to begin warrantless surveillance. That was the date on which Congress promulgated the Authorization for Use of Military Force, which the administration considers a declaration of war against Al Qaeda. Yet the need for such surveillance was at its most acute on September 11. And, if a war is raging inside the United States on the sixteenth day after an invasion begins and it is a matter of military necessity to continue warrantless interceptions of enemy communications with people in the United States, would anyone think the 15-day rule prohibitive?

We must not ignore the costs to liberty and privacy of intercepting phone calls and other electronic communications. No one wants strangers eavesdropping on his personal conversations. And wiretapping programs have been abused in the past. But, since the principal fear most people have of eavesdropping is what the government might do with the information, maybe we can have our cake and eat it, too: Permit surveillance intended to detect and prevent terrorist activity but flatly forbid the use of information gleaned by such surveillance for any purpose other than to protect national security. So, if the government discovered, in the course of surveillance, that an American was not a terrorist but was evading income tax, it could not use the discovery to prosecute him for tax evasion or sue him for back taxes. No such rule currently exists. But such a rule (if honored) would make more sense than requiring warrants for electronic surveillance.

Once you grant the legitimacy of surveillance aimed at detection rather than at gathering evidence of guilt, requiring a warrant to conduct it would be like requiring a warrant to ask people questions or to install surveillance cameras on city streets. Warrants are for situations where the police should not be allowed to do something (like search one's home) without particularized grounds for believing that there is illegal activity going on. That is too high a standard for surveillance designed to learn rather than to prove.

**[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*.**

## RELATED LINKS

[Character Flaw](#)  
Bush's new humility **TNRD**  
[Rebel Quelled](#)

[The Insider](#)  
Bush and the GOP scandals **TNRD** web only  
[Spy Crimes](#)

Suddenly, Bush just wants to be liked

[Breakfast at Epiphanies](#)

Bush officials are frequently misunderstood. Allow them to clarify web only

The president's domestic wiretapping program is illegal [Con Text](#)

Bush's new strategy for defending the war? Take Democratic quotes out of context **TNRD** web only

[Home](#) | [Politics](#) | [Books & the Arts](#) | [Legal Notices](#)  
[Privacy Policy](#) | [Contact TNR](#) | [Subscriber Services](#) | [Advertise With Us](#)  
Copyright 2006, The New Republic





Searching for the perfect mix.



THE  
**NEW REPUBLIC**  
**ONLINE**









THIRD



THIRD

THIRD

