

# The New Domestic Surveillance Regime: Ineffective Counterterrorism That Threatens Civil Liberties and Constitutional Separation of Powers

Kate Martin\*

*Secret intelligence failed to provide reliable information and knowledge for the weighty decision of when and against whom to go to war. Nevertheless, it is being touted as the be-all and end-all for targeting Americans at home for surveillance, imprisonment and black-listing. Is there any basis for hoping that it will prove more effective at protecting the national security at home, including civil liberties, than it proved to be when deciding to invade Iraq?*

## I. INTRODUCTION

On August 16, 2007, the *Washington Post* ran a story about the Defense Department agreeing that the Department of Homeland Security could use military spy satellites for aerial surveillance of the interior of the United States (“U.S.”). The same day the paper ran a separate story, quoting a Rand Corporation terrorism expert asserting that there was no evidence of “a significant cohort of terrorist operatives” in the U.S.<sup>1</sup> These two stories illustrate a troubling development: the reach of the intelligence activities now being directed against Americans far exceeds the small number of terrorists who have been charged or are even suspected of being here. Since then, for example the National Security Agency (“NSA”) has just been granted vast new surveillance powers over Americans’ international communications.

If there are at most a handful of terrorist cells in the U.S., one must ask why has the Administration decided to use its expensive satellite capabilities and other scarce intelligence resources in this way?

The answer can be found by comparing the record of massive expansion of secret domestic intelligence authorities and the explosion of technological surveillance capabilities since 9/11 with the history of arrest and imprisonment of hundreds of individuals in the U.S. since then as part of the Administration’s “War on Terror.” Those imprisoned include both citizens and non-citizens, almost all Muslim; some have been convicted of minor crimes, fewer of terrorism-related crimes, but many more were never even charged with any crime.

---

\* Director, Center for National Security Studies.

<sup>1</sup> Joby Warrick, *Domestic Use of Spy Satellites to Widen*, WASHINGTON POST, Aug. 16, 2007. Dan Eggen, *Terror Threat Grows Quietly, Report Warns*, WASHINGTON POST, Aug. 16, 2007.

The expansion of secret surveillance authorities used domestically is integral to the Administration's declaration that the U.S. is at war and that intelligence is the most important weapon for winning this war. The connections between such surveillance and the arrests and detentions of individuals identified primarily on the basis of their religious beliefs have not been adequately examined. The question posed most often today is what kind of oversight and safeguards can we build to prevent abuses of these new surveillance powers? But the question is usually asked in too narrow a context—without looking at the record of domestic detentions—and with little appreciation for the historical record of the abuses of secret domestic intelligence authorities by all governments, both democratic and totalitarian.

Before 9/11, there was a wide recognition of and effort to mitigate the substantial risks posed to democracy and human rights by secret domestic intelligence activities. As a civil liberties lawyer working on government surveillance and other national security issues for 13 years before 9/11, I frequently reassured activists that the government was not spying on them, unless they worked for pro-Palestinian causes, in which case the Federal Bureau of Investigation ("FBI") had a Foreign Intelligence Surveillance Act ("FISA") warrant. There was also healthy skepticism about the effectiveness of such activities in preventing terrorist acts. That broad perspective has largely disappeared, however, and been replaced by much narrower analyses of the potential risks and benefits of particular surveillance techniques.

Today we must ask whether the U.S. is in danger of becoming a place where the government's knowledge gives it too much power over individual lives and, if so, how can that be prevented. I hope I am wrong, but I can no longer find any reason to give this Administration or the intelligence agencies and their leaders the benefit of the doubt in worrying about such threats to our democracy.

To be clear, I do not dispute the threat of additional violent attacks inside the U.S. or that the government should use appropriate surveillance and investigative techniques to attempt to identify and locate individuals planning such attacks before they happen. However, it would be both ineffective and dangerous to create a domestic intelligence agency with virtually unrestrained power to conduct national security surveillance inside the U.S. Instead, we need a strong agency with law enforcement responsibilities, including prevention, which is trained to carry out targeted investigations within constitutional rules, to prevent international terrorist plots. Whether such responsibility should remain with the FBI or a new agency established under the control of the Department of Justice is another question. I note with some relief that, to date, suggestions to establish a domestic intelligence agency have been rejected.

But there is increasing evidence that an enormous domestic intelligence capability is, in fact, being built piece-by-piece, much of it housed in the Department of Defense, including the NSA. The satellite surveillance, though vast, is only a small piece of that. In order to evaluate the benefits and risks of this expansion of domestic intelligence, it is necessary to start with some of the general characteristics of secret intelligence.

## II. THE RISKS OF SECRET DOMESTIC SURVEILLANCE

What differentiates "intelligence" from any other human endeavor to attain information and knowledge is that it is conducted by the state in secret. This paper addresses only secret intelligence activities carried out inside the U.S. and directed against U.S. citizens and residents. Such activities, unlike intelligence directed overseas, impact directly on the compact between the government and the governed. Indeed, secrecy poses difficulties for intelligence agencies themselves. Long-time CIA veteran

and Director William Colby explained, in connection with ensuring the agency's survival in the mid-1970s in the face of intense public outrage over past abuses:

The Agency's survival, I believed could only come from understanding, not hostility, built on knowledge, not faith....

The CIA no longer could operate within the traditions of the past. The CIA must build, not assume, public support, and it can do this only by informing the public of the nature of its activities and accepting the public's control over them. It must convince the people that it is not some nefarious "invisible government" engaged in heinous crimes and oblivious to American democratic values, but a legitimate, controlled, and immensely valuable weapon in the arsenal of our democracy, serving to protect the nation and promote its welfare....

The only way we can have such a public [supportive of the intelligence community] is by making the CIA an integral part of our democratic process, subject to our system of checks and balances among the Executive and the Congress and the Judiciary, responsive to the Constitution and in the end controlled by the informed populace it serves.<sup>2</sup>

While this vision was not fully implemented by past administrations, there is no evidence that the current Administration understands that this point applies to the intelligence community in spades when it turns its activities on Americans.

Secret intelligence-gathering and the corresponding lack of transparency also greatly increase the probability of error. Moreover, because intelligence is by its nature secret, it is difficult to design mechanisms and systems that provide any real and effective oversight or accountability. Yet, the secret intelligence agencies are perhaps the agencies most in need of oversight and accountability both because of the risks they pose to democratic decision-making and because the government gains enormous power over individuals through knowledge about those individuals. As Senator Sam Ervin, chief author of the Privacy Act, wrote in 1974:

[D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.

...

---

<sup>2</sup> WILLIAM H. COLBY, HONOURABLE MEN 21(1978).

Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.<sup>3</sup>

Since 9/11, however, it is widely claimed that secret surveillance and intelligence against Americans is essential to our national security. Providing for our national security is certainly an essential function of our federal government, but this approach raises serious questions. Is the U.S. building a surveillance regime likely to be effective at stopping terrorist attacks? Or, is it constructing a surveillance regime likely to become an ungovernable tool in the hands of an executive for use against its own citizens, serving the purposes of those in power rather than the national interest as constitutionally and democratically determined?

We need to know much more in order to have any confidence about the answers to these questions. We must understand the underlying rationale for the surveillance, the ways in which it may be used, and just what such surveillance entails.

### III. “WE’RE AT WAR.” THE JUSTIFICATION FOR DOMESTIC INTELLIGENCE

This claim and its corollary—that intelligence is the most important weapon in this war—are the key rationales for the current surveillance regime. Understanding this is critical to assessing the risks and benefits of the regime in terms of constitutional requirements and effective counterterrorism.

This claim underlies the assertion by the Administration that the President has Article II Commander in Chief powers, authorizing him to override statutory prohibitions—in secret—without informing the Congress or the American people.<sup>4</sup> Such powers are said to encompass surveillance of the enemy—wherever found and however identified. The Administration reads the Fourth Amendment to require only that surveillance inside the U.S. against U.S. citizens and residents be “reasonable” and it claims that the executive branch is the sole judge of reasonableness.

While courts have on occasion approved warrantless surveillance, there is a key difference between the surveillance approved in those cases and the secret surveillance being conducted for intelligence purposes. In each of those cases, the target of the search or seizure knew that his belongings had been searched or that his communications were overheard and, therefore, could challenge the reasonableness of the search with a judge as the final arbiter. The essence of the “wartime” surveillance being conducted by the Bush Administration in the U.S. against U.S. citizens and residents is

---

<sup>3</sup> Senator Ervin, Speech introducing S. 3418 (June 11, 1974), *reprinted in* COMMITTEE ON GOVERNMENT OPERATIONS, UNITED STATES SENATE AND THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S.3418, at 157 (Public Law 93-579)(Sept. 1976) (hereinafter SOURCE BOOK ON PRIVACY).

<sup>4</sup> These Article II claims are outlined in a variety of sources. *See e.g.* Memorandum from Off. Legal Counsel to Att’y Gen. Alberto Gonzales (Aug. 1, 2002); Dep’t of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006) (White paper on FISA surveillance); Letter from Bryan Cunningham to Arlen Specter & Patrick Leahy (Feb. 3, 2006); JOHN YOO, *WAR BY OTHER MEANS, AN INSIDER’S ACCOUNT OF THE WAR ON TERROR* 2006.

that it remains a secret and may never be revealed to those who have been spied on. Further, its reasonableness is never reviewed by a court in an adversarial proceeding. Indeed, when individuals have attempted to challenge such surveillance, the government has strongly argued against judicial review.<sup>5</sup>

Other Administration supporters argue for secret warrantless surveillance not by claiming extraordinary Article II powers for the President, but instead by reading the protections of the Bill of Rights to incorporate a balancing test. They claim that individual rights must be balanced against national security concerns and that the risk of terrorist attacks outweighs the protections and checks and balances traditionally understood to be guaranteed by the Constitution.<sup>6</sup>

These claims have led to adoption of a military model of surveillance, even when directed inside the U.S. against U.S. citizens. As explained by John Yoo, author of the Justice Department's legal opinions approving the use of warrantless surveillance against Americans in violation of FISA: "Individualized suspicion [as required by the Fourth Amendment] does not make sense when the purpose of intelligence is to take action, such as killing or capturing members of the enemy, to prevent future harm to the nation from a foreign threat."<sup>7</sup> The same arguments are also advanced to defend a military model of detention without charge or trial for individuals seized in the United States as "enemy combatants." The more benign formulation of this claim is that because it is difficult to find Al Qaeda in this country, the threat is so great, and there is no real harm to privacy interests from the kind of surveillance at issue, secret warrantless surveillance of Americans is therefore justified and constitutional.

Both formulations rest on an unexamined and unsupportable hope that surveillance will actually work, while ignoring its real harms. Before examining both of those flawed premises, let us look more closely at the purpose of such surveillance, what it includes, and how is it carried out.

#### IV. DOMESTIC "WARTIME" SURVEILLANCE AND DETENTION

There is much we still do not know about the connections between the Patriot Act amendments to FISA, the warrantless NSA surveillance program revealed in December 2005, and the Administration's claim of authority to imprison Americans and others seized in the U.S. as "enemy combatants" without charges, trial, or even any access to counsel or any court for months on end. It is clear that the Bush Administration viewed both detention and secret surveillance as weapons to be employed against the "enemy" both here and abroad. In the months following 9/11, more than 1,000 individuals were arrested in secret, physically assaulted in custody, and held illegally for months on end, simply because they were (or were believed to be) Arabs or Muslims. Then-Attorney General Ashcroft repeatedly spoke about "sleeper cells" in the U.S. Ashcroft ordered prosecutors to comb through years of pre-9/11 FISA surveillance to determine what criminal charges could be brought on the basis of the old surveillance tapes and some prosecutions of Arabs, Muslims and Palestinians resulted. And the President claimed the extraordinary and unprecedented authority to command the military to seize U.S. citizens and legal residents in the United States, imprison them

---

<sup>5</sup> Providing for a FISA court order to initiate such surveillance does not address this issue, as such orders are issued in *ex parte* proceedings.

<sup>6</sup> See e.g. RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY (2006).

<sup>7</sup> Yoo, *supra* note 4, at 112.

incommunicado for years, without access to a lawyer or any judicial review on the claim that they were “enemy combatants.”

There is no doubt that the secret surveillance both under FISA and by the NSA in violation of FISA was part of this system whereby the government would gather information in secret, and use it to seize and imprison Americans as enemy combatants. It seems evident that many in the Administration contemplated from the beginning that the government would use warrantless surveillance outside the law to “disable” or “take out” individuals in the U.S. suspected of terrorist associations. When the legal opinions justifying the warrantless wiretapping program are finally disclosed, we will know whether they expressly discuss this objective. The system of secret intelligence gathering to find Al Qaeda “sleeper cells” is not designed to “disable” suspected terrorists found in the United States by bringing criminal charges resulting in imprisonment or immigration charges resulting in detention followed by deportation. To the contrary, it was expressly designed to enable the government to detain individuals without any due process as “enemy combatants.” It was also designed in order to allow the seizure of non-citizens and render them outside any legal process to countries where they could be held outside the law and interrogated with no protection against being tortured. Thus, there is a deep and important connection between the use of secret surveillance with no outside checks and the system of detaining individuals outside the legal protections (such as they are) of the criminal and immigration systems.

In both cases, the Administration dismisses any care for constitutional norms because they calculate that such norms must give way in the face of current threats. Their defense of secret surveillance rests less on the claim that the surveillance will not be used against individuals and more on the assurance that it will only be used against guilty individuals with no need for the innocent to worry. But the determination of the guilt or innocence of those accused is shrouded in secrecy and is no longer tied to any due process.

Is this description exaggerated? Has this actually happened? There is no doubt that the legal analysis proffered by the Administration for its claim of authority to detain “enemy combatants” and to engage in extraordinary rendition of individuals outside the legal process to countries of its choosing rests on the same assumptions and adopts the same reasoning as the legal analysis proffered in support of secret warrantless surveillance in the U.S., even when prohibited by statute. While at this time there are only two known instances of individuals seized in the U.S. and held without charges as enemy combatants and one extraordinary rendition from the U.S., there are many instances of individuals kidnapped around the world and held in secret without any process. It is not known what role secret, warrantless surveillance played in these cases, because the government has refused to say. But it appears that Ashcroft was most likely referring to warrantless NSA wiretaps when he first outlined the government’s allegations against the U.S. citizen Jose Padilla, who was seized in the U.S. and detained as an enemy combatant for more than three years.<sup>8</sup>

The claim that the Administration has the authority to conduct warrantless secret surveillance because the U.S. is at war has other important consequences as well: the Defense Department has become heavily involved in domestic surveillance activities and the government has violated the due process rights of individual criminal

---

<sup>8</sup> Jose Padilla eventually obtained a lawyer and filed a habeas corpus petition challenging his detention as an enemy combatant. While that petition was before the courts, the government suddenly transferred him from military detention and brought criminal charges against him. He was tried in 2007 and convicted.

defendants, who have been denied access to information about government surveillance of them.

As far as I have been able to determine, in all the criminal cases where the defendants have sought to discover whether they were listened to by the NSA, the government has refused to say and has won on the grounds that the information should be kept secret, notwithstanding the protective procedures available under the Classified Information Procedures Act. One might wonder what is secret, once the subject of the surveillance is in prison? But more importantly, allowing the government to withhold such information from a defendant violates his or her Fourth Amendment and basic due process rights. Prior to the NSA warrantless surveillance program, it was the established understanding that when the government indicted an individual, it was required to disclose whether he had been wiretapped and to make available to him the transcripts of such wiretaps as a matter of fundamental due process. Such an after-the-fact check traditionally provided the only adversarial judicial review of whether secret surveillance was, in fact, lawful.

Less attention has been paid to the civil liberties issues raised by criminal prosecutions of Muslim-Americans (including a number of Imams) than has been paid to the enemy combatant detentions. But there are serious issues about whether illegal surveillance is being used to target individuals on the basis of their constitutionally-protected religious activities. Questions have been raised about sting operations used to entrap individuals who may have been targeted based on warrantless surveillance.<sup>9</sup> Individuals have also been charged, not with attempted terrorist attacks, but with much more inchoate offenses, for example under material support laws. This comes dangerously close, in the words of Professor Peter S. Margulies, to “allow[ing] someone to be found guilty for something that is one step away from a thought crime.”<sup>10</sup>

## V. THE GOVERNMENT IS ENGAGED IN A MULTI-BILLION DOLLAR EFFORT TO BUILD A MASSIVE WEB OF DOMESTIC INTELLIGENCE CAPABILITIES

While there has been extensive public debate and some limited congressional oversight on the warrantless NSA spying, some provisions of the Patriot Act, and some aspects of data-mining, there has been little public information about or congressional understanding of the overall effects of the massive increases in surveillance capabilities. There likewise has been little debate about or oversight of the extensive re-writing of legal restrictions to weaken the checks on employing these surveillance capabilities against U.S. citizens and residents.

There has been a massive shift from surveillance and intelligence-gathering based on a factual predicate—such as specific information or a lead about a suspicious person or event—to surveillance and intelligence-gathering intended to obtain vast troves of data on millions of people. The NSA has been given authority to acquire and analyze the international calls and e-mails of Americans in the U.S., an intelligence activity that was formerly conducted by the FBI. The latter traditionally investigated based on some factual predicate; the NSA “vacuums” information in the hope that it may be useful in the future. Turning the NSA’s supercomputing capabilities inward on Americans, when they were previously directed outward towards foreigners overseas,

---

<sup>9</sup> Adam Liptak, *Spying Program May Be Tested by Terror Case*, NEW YORK TIMES Aug. 26, 2007.

<sup>10</sup> Adam Liptak, *Padilla Case Offers New Model of Terrorism Trial*, NEW YORK TIMES Aug. 18, 2007.

is an enormous change. In addition, the intelligence agencies not only collect, but also retain billions of items of data on Americans on the theory that they may be useful in the future, including data gathered by commercial entities as well as that collected by the government directly.

Here are some other key aspects of these developments:

- Data-mining—the use of enormous computing capabilities to aggregate enormous amounts of data and analyze and search the data using a limitless number of search algorithms.
- Much greater involvement by the Defense Department, both through its intelligence agencies and the Northern Command, in domestic intelligence, including the analysis of data collected by other agencies and other efforts like the use of military satellites over the U.S. to collect data directly.
- Massive initiatives to make myriad government databases available to thousands of government officials, including state and local police, CIA officials, and White House personnel. Notably these mass information-sharing efforts lack any attempt to train personnel on what is important and relevant information. It would seem that those who collect the information and know something about its source would generally be in the best position to assess its importance, but little attention is paid to that issue. Nor is there any real effort to assure that those who need specific information actually receive it, rather than simply warehousing the information in massive data-bases accessible to thousands of individuals.
- The elimination of legal rules intended to provide safeguards against abuse, *e.g.* the Patriot Act amendment permitting wholesale sharing of criminal wiretap intercepts of Americans with intelligence and White House personnel with no judicial oversight or audit mechanism.
- An attempt to eliminate meaningful judicial review of surveillance, either by claiming that no judicial determination of individualized probable cause is required to initiate surveillance or that there should be no after-the-fact judicial review of such.
- The creation of secret “watchlists” containing names of thousands of Americans, without any defined or legitimate purpose for such lists, much less criteria for inclusion or protections against abuse.
- Discriminatory data collection based on perceived religious affiliation or ethnicity, such as the request by the Department of Homeland Security for census data on neighborhoods with high concentrations of Arab-American residents and the program to collect data from Middle Eastern residents in the U.S. concerning their contacts and associates in the U.S.
- Fifteen thousand “confidential human sources” a.k.a. “informants” employed by the FBI, including an unknown, but apparently quite substantial, number working on counterterrorism (to find the handful of terrorists) and directed to infiltrate mosques or civic organizations.
- Changes in agency rules to allow intelligence agents to freely attend and record information about religious services or public political meetings.



In sum, as one proponent of increased surveillance describes it, the government is on its way “to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched. It should soon be possible—maybe it is already possible—to create a comprehensive electronic dossier for the vast majority of American adults... [and that] digitized dossier would be continuously updated.”<sup>11</sup> It is not clear whether this is being done on the assumption that it is useful to employ limited resources in this way, even though most people are innocent, or with a more sinister understanding that (as purportedly observed by Stalin’s KGB chief) “show me the man and I’ll show you the crime.”

The Administration claims that building such surveillance capabilities is crucial for effective counterterrorism and holds few risks for civil liberties. But the claim that it has been or will be effective is backed only by hypotheticals. To date, there has been no demonstration that such surveillance is likely to yield crucial information and no examination of whether the intelligence agencies are competent or knowledgeable enough to recognize what is crucial and to use such data to stop terrorists, assuming the data can even be found.

The public record supplies little reason for confidence that the intelligence agencies will use their increased surveillance capabilities wisely. The intelligence community knew before 9/11 of the threat that Al Qaeda posed to the U.S. and that Al Qaeda associates were in the U.S. It did not recognize the significance of the information it had nor did it know what steps to take. That failure was followed by the failures of intelligence used to make the case for war in Iraq. The pre-9/11 record can be read as failures of analysis: the agencies had too much information and not enough understanding of its significance. They are now engaged in gathering oceans of information on innocent people with no explanation about how they will now differentiate the significant from the unimportant.

While there have been many legal and bureaucratic changes made since 9/11 and politicians have claimed that such changes have prevented more attacks in the U.S. since then, there has been no objective study or analysis to evaluate those claims. One of the key questions that needs to be asked is whether any useful information that may have been obtained, for example through warrantless NSA surveillance, could have been obtained lawfully, through less intrusive means, *e.g.* with a warrant.

Nor has there been any comprehensive examination of what uses have been made of the information collected through these massive efforts. To the contrary, the Administration has repeatedly rebuffed any efforts to discover even limited aspects of its activities. There has been no examination of what uses the government has made of such information to watch list Americans, to target individuals for further investigation or prosecution, or to prosecute them. Such examination, for example, would need to go beyond the political claims made by the Administration concerning the importance of its terrorism prosecutions since 9/11. At least some of those have targeted individuals who seem highly unlikely to possess the ability or intention to carry out mass murder. Other prosecutions were brought on the basis of wiretapping authorities that existed before 9/11. For example, the prosecutions of the defendants in Lackawanna were based on FISA wiretaps carried out years before 9/11.

Moreover, there is no country in the world where domestic intelligence collected in secret has not been misused by the government in power, usually against its political opponents for its own political gains. In response to this charge, the Administration

---

<sup>11</sup> POSNER, *supra* note 6 at 135.

argues that the risks to civil liberties are diminished because much of the massive amounts of data is initially “read,” collected, analyzed and sorted by machine, rather than by a person. They argue that civil liberties will be protected by built-in technological protections against the loss or theft of the data and against rogue government agents “misusing” such information. Both arguments ignore the real civil liberties risks—the authorized use of such data stored in and retrieved by computers—against individuals on the orders of government officials, now or for the indefinite future, in violation of basic constitutional rights. The risks include: targeting and discriminating against individuals on the basis of their religion or ethnicity; using information against political opponents or unfairly to deny individuals jobs; using information obtained in violation of the Fourth Amendment against them; or detaining individuals arbitrarily, without charge, and with no due process. We have already seen the Joint Terrorism Task Forces, including agents from the FBI, CIA and Defense Department, collect information on the Quakers and other religious groups with absolutely no connection to terrorism, merely because they opposed the U.S. war in Iraq.

## VI. RECOMMENDATIONS

First, and perhaps most importantly, the war model should be rejected as a legal framework for surveillance directed against individuals in the United States. Second, both Congressional and public scrutiny are needed to determine whether individuals are being targeted on the basis of their First Amendment-protected religious activities. Third, wiretapping and physical searches of individuals in the U.S. should remain secret for only a limited period of time; thereafter the individuals whose belongings have been searched or communications seized must be notified by the government, with limited exceptions upon a specific finding of necessity by a court.

More broadly, many have urged adoption of adequate safeguards and oversight to prevent abuses. While superficially appealing, such a recommendation does not address a fundamental question: Are the powers being amassed by the government so great that oversight will not be sufficient, that traditional mechanisms should not be counted upon to protect the constitutional system in a time of crisis? This question cannot be answered without much more information about what is currently being done.

Congress needs to conduct a comprehensive in depth examination of the whole of domestic intelligence activities, to see how the different activities in different agencies fit together, to examine how the information is being used and how it may be used in the future. Such examination should be conducted not just by the Intelligence committees, but also by the Judiciary and perhaps Homeland Security committees operating jointly. As much information as possible should be made public and there should be a comprehensive and detailed public report issued by the committees.

The inquiry should start with an open question about the design or efficacy of oversight and accountability mechanisms. The inquiry should ask first whether some powers should ever be granted to the government; whether the law or institutional safeguards can ever be adequate to protect constitutional government and individual liberties against the kind of power a government will amass when it harnesses all potential technological surveillance capabilities.

The words of Senator Church from 30 years ago are even more relevant today. “I don’t want to see this country ever go across the bridge,” Senator Church said. “I know the capacity that is there to make tyranny total in America, and we must see to it that [the National Security Agency] and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.”<sup>12</sup>

---

<sup>12</sup> *Meet the Press*, (NBC television broadcast Aug. 17, 1975); quoted in James Bamford, *Big Brother is Listening*, THE ATLANTIC MONTHLY, April 1, 2006.