



October 12, 2007

Chairman John D. Dingell  
Ranking Member Joe Barton  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

Chairman Edward J. Markey  
Ranking Member Fred Upton  
Subcommittee on Telecommunication and the Internet  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

AMERICAN CIVIL  
LIBERTIES UNION  
WASHINGTON  
LEGISLATIVE OFFICE  
915 15th STREET, NW, 6<sup>TH</sup> FL  
WASHINGTON, DC 20005  
T/202.544.1681  
F/202.546.0738  
[WWW.ACLU.ORG](http://WWW.ACLU.ORG)

Caroline Fredrickson  
DIRECTOR

NATIONAL OFFICE  
125 BROAD STREET, 18<sup>TH</sup> FL.  
NEW YORK, NY 10004-2400  
T/212.549.2500

OFFICERS AND DIRECTORS  
NADINE STROSSEN  
PRESIDENT

ANTHONY D. ROMERO  
EXECUTIVE DIRECTOR

RICHARD ZACKS  
TREASURER

Chairman Bart Stupak  
Ranking Member Edward Whitfield  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairmen and Ranking Members:

The American Civil Liberties Union, its hundreds of thousands of members and 53 affiliates nation-wide respectfully submit our views on the potential security and privacy implications of the Protect America Act of 2007 (Pub. Law 110-55) (hereinafter PAA), as requested in the Chairmen's letter of October 2, 2007. The intelligence community in general and the National Security Agency (NSA) in particular have long histories of abusing their authority whenever their exercise of power is not carefully monitored, and the record has shown that such abuses have rarely led to actual increases in security.

The Federal Bureau of Investigation's (FBI) COINTELPRO program, the Central Intelligence Agency's (CIA) Operation CHAOS and the NSA's Project SHAMROCK are only a few of the infamous domestic intelligence collection programs uncovered by the 1975 Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee).<sup>1</sup> The discovery of these misguided programs led Congress to enact significant reforms designed to increase both the

---

<sup>1</sup> Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate, 94<sup>th</sup> Cong., Final Report on Supplemental Detailed Staff Reports on Intelligence Activities and the Rights of Americans (Book III), S. Rep. No. 94-755, (1976).

accountability and the effectiveness of the intelligence agencies. Foremost among these reforms was the Foreign Intelligence Surveillance Act of 1978.<sup>2</sup>

Unfortunately, the increased fear of terrorism, or more specifically the fear of undetected terrorist “sleeper cells” has led to a new series of secret surveillance and data collection programs that are based not on reasonable suspicion, but rather on an unproven theory that asymmetric threats to our security can be detected and countered through massive data collection efforts coupled with predictive data mining technology.

In December of 2005 the *New York Times* revealed that shortly after the 9/11 attacks the NSA began conducting warrantless domestic eavesdropping in violation of the FISA and the U.S. Constitution.<sup>3</sup> The Bush administration acknowledged approving this surveillance as part of a program it called the Terrorist Surveillance Program (TSP). Subsequent articles in the *Times* and *USA Today* alleged that major telecommunications companies “working under contract to the NSA” were also providing the domestic call data of millions of Americans to the government for “social network analysis.”<sup>4</sup> But the information collected with these NSA warrantless wiretapping programs was reported to have been of little value to FBI investigators.<sup>5</sup>

The Bush administration later submitted the TSP, or some version of it, to the Foreign Intelligence Surveillance Court (FISC) for approval in January of 2007, but months later a second FISC judge reportedly decided the TSP could not be renewed as constituted, which initiated an intense lobbying effort that resulted in the passage of the PAA.<sup>6</sup> Director of National Intelligence Michael McConnell was quick to claim success with the new powers granted under the PAA, claiming in Congressional testimony they were useful in interdicting a terrorist plot in Germany, but this claim was later discovered to be untrue.<sup>7</sup> That DNI McConnell was unable to point to any real successes of this program begs the question of whether such programs actually improve the national security.

## MASS DATA COLLECTION PROGRAMS NOT EFFECTIVE FOR SECURITY

---

<sup>2</sup> 50 U.S.C. §1801, *et. seq.* (1978).

<sup>3</sup> James Risen and Eric Lichtblau, *Bush lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, available at <http://www.nytimes.com/2005/12/16/politics/16program.html?ei=5090&en=e32072d786623ac1&ex=1292389200>.

<sup>4</sup> Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at 1A, available at [http://www.usatoday.com/news/washington/2006-05-10-nsa\\_x.htm](http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm). See also, James Risen and Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times, Dec. 24, 2005.

<sup>5</sup> Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta, Jr., *Spy Agency Data After Sept. 11 Led FBI to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1, available at <http://www.nytimes.com/2006/01/17/politics/17spy.html?ei=5090&en=f3247cd88fa84898&ex=1295154000&pagewanted=print>.

<sup>6</sup> Michael Isikoff and Mark Hosenball, “Behind the Surveillance Debate,” *Newsweek*, Aug. 1, 2007, at: <http://www.msnbc.msn.com/id/20075751/site/newsweek/page/0/>

<sup>7</sup> Michael Isikoff and Mark Hosenball, “Spy Master Admits Error,” *Newsweek*, Sept. 12, 2007, at: <http://www.msnbc.msn.com/id/20749773/site/newsweek/>

Indeed there is little evidence to suggest the NSA programs authorized by the PAA, or any other data surveillance and mining programs can be effective in predicting or preventing terrorist behavior, and relying on them may simply waste finite security resources. Soon after 9/11, Gilman Louie, the head of In-Q-Tel, warned against a “data mining or profiling” approach to counterterrorism, which he described as “too blunt an instrument” to be a primary tool of surveillance.<sup>8</sup> In a 2003 letter opposing the Defense Department’s proposed data mining program known as Total Information Awareness (TIA), the Association for Computing Machinery expressed serious doubts about the feasibility of such data surveillance programs, which they said,

...suffer from fundamental flaws that are based in exceedingly complex and intractable issues of human nature, economics and law. . . . As computer scientists and engineers we have significant doubts that the computer-based TIA Program will achieve its stated goal of “countering terrorism through prevention.” Further, we believe that the vast amount of information and misinformation collected by any system resulting from this program is likely to be misused to the detriment of many innocent American citizens.<sup>9</sup>

And in a recent CATO Institute Policy Analysis, Jeff Jonas and Jim Harper explained that while data mining has many useful purposes in other applications, it is poorly suited for predicting or preventing acts of terrorism:

It would be unfortunate if data mining for terrorism discovery had currency within national security, law enforcement, and technology circles because pursuing this use of data mining would waste taxpayer dollars, needlessly infringe on privacy and civil liberties, and misdirect the valuable time and energy of the men and women in the national security community.<sup>10</sup>

Data mining will not work in terrorism investigations because data mining is all about the data, and as Jonas and Harper point out, “terrorism does not occur with enough frequency to enable the creation of valid predictive models.”<sup>11</sup> Without valid predictive models such a system will invariably produce high numbers of false positives, placing innocent Americans under a cloud of suspicion that diverts resources from focusing on true threats to our security. The Joint House-Senate Intelligence Committee investigation into the terrorist attacks of 9/11 found that significant pieces of information relevant to the attacks

---

<sup>8</sup> Steve Lohr, *Data Expert is Cautious About Misuse of Information*, N.Y. TIMES, Mar. 25, 2003, at C6, available at <http://query.nytimes.com/gst/fullpage.html?sec=technology&res=9E07E6D71530F936A15750C0A9659C8B63>

<sup>9</sup> Letter from Association for Computing Machinery Public Policy Committee to Sens. John Warner and Carl Levin (January 23, 2003), available at [http://www.acm.org/usacm/Letters/tia\\_final.html](http://www.acm.org/usacm/Letters/tia_final.html).

<sup>10</sup> Jeff Jonas and Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, CATO INSTITUTE POLICY ANALYSIS, Dec. 11, 2006, at 1, <http://www.cato.org/pubs/pas/pa584.pdf>.

<sup>11</sup> Jonas and Harper, *supra*, at 8.

were overlooked in the “vast streams” of intelligence being gathered.<sup>12</sup> Data surveillance and collection programs which are not focused on individuals reasonably believed to be involved in improper activity only collect massive amounts of irrelevant information, making it more difficult to find the few pieces of information that are useful to defending our national security.

Congress has been stonewalled in its attempts to get more information regarding the scope of the NSA’s post-9/11 programs, but a recent audit by the Department of Justice Inspector General (IG) documents the abuse of a similar domestic intelligence collection program at the FBI.<sup>13</sup> Perhaps not surprisingly, the Inspector General found widespread misuse of FBI’s expanded power to collect telephone and financial records using National Security Letters (NSLs) under authorities granted in the USA PATRIOT Act.<sup>14</sup> Between 2003 and 2005 the FBI issued over 143,000 NSL requests (the true number of requests is unknown because the FBI did not keep adequate records), often without even opening corresponding investigations. The IG report indicates that FBI personnel developed “close working relationships with private sector companies, including telephone companies that furnished points of contact to facilitate the FBI’s access to records held by these companies.”<sup>15</sup> This familiarity facilitated a breakdown of the formal legal process, which allowed the FBI and the company employees to circumvent privacy laws by obtaining telephone and financial records using illegal “exigent letters” and “certificate letters” instead of duly authorized grand jury subpoenas or NSLs.

Like the data reportedly collected by the NSA, the IG found that the information illegally collected through the improper use of NSLs was dumped into huge FBI databases for analysis, including an Investigative Data Warehouse containing over 560 million records.<sup>16</sup> Yet despite such aggressive collection efforts, the IG was only able to document one material support for terrorism conviction resulting from the FBI’s use of NSLs.<sup>17</sup> Further, the abuse of this NSL authority yield no prosecutions, let alone convictions, for activity to plan a terrorist attack. Thus, the effectiveness of massive data mining programs must be called into question. These results are, unfortunately, all too typical.

Intelligence collection efforts that are not based upon reasonable suspicion of wrongdoing do not improve our level of security; they only produce irrelevant piles of data and bloated watchlists. An October, 2006 segment of the CBS News magazine “60 Minutes” lampooned the 44,000-name No-Fly list for, among other obvious errors and

---

<sup>12</sup> Joint Inquiry into Intelligence Committee Activities Before and After the Terrorist Attacks of Sept. 11, 2001, Report of the Senate Select Committee on Intelligence and the U.S. House Permanent Select Committee on Intelligence, S. Rep. 107-351, H. Rep. 107-792, (Dec. 2002).

<sup>13</sup> DEP’T. OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS (March 2007), <http://www.usdoj.gov/oig/special/s0703b/final.pdf> [hereinafter NSL Report].

<sup>14</sup> The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Pub. Law 107-56).

<sup>15</sup> NSL Report, at 87.

<sup>16</sup> *Id.*, at 30, footnote 64.

<sup>17</sup> *Id.*, at 64.

omissions, still containing the names of 14 of the 19 hijackers killed during the September 11, 2001 terrorist attacks.<sup>18</sup> Yet the no-fly list is dwarfed by the FBI's Terrorist Screening Center's (TSC) watchlist, which contains over 720,000 records and increases by an average of 20,000 records per month.<sup>19</sup> A recent Department of Justice IG audit determined the TSC watchlist to be inaccurate and error-prone, noting that several known or suspected terrorists were not watchlisted appropriately and that 38 percent of the records tested "continued to contain errors or inconsistencies that were not identified through the TSC's quality assurance efforts," thereby increasing "the chances of innocent persons being stopped or detained during an encounter because of being misidentified as a watchlist identity."<sup>20</sup> Highlighting the fact that such bloated watchlists do nothing to improve security, a recent report by the *Washington Post* indicates even this inappropriately long list has produced few arrests.<sup>21</sup>

The failure of these massive data collection, mining, and analysis programs to yield positive results has very serious consequences for both our national security and our liberty. As the 2007 National Intelligence Estimate reveals, the United States is still susceptible to attack from persistent and motivated terrorists, but despite the unprecedented scope of these data collection programs and the resources devoted to them, the government has made relatively few significant terrorism arrests and prosecutions.<sup>22</sup> Data produced by the Executive Office of United States Attorneys and analyzed by the Transactional Records Access Clearinghouse (TRAC) reveals that in 2006 the Department of Justice declined to prosecute a full 87% of the international terrorism cases the FBI referred for prosecution, making painfully evident that the bulk of the FBI's counterterrorism efforts are completely for naught.<sup>23</sup> And despite the increased levels of surveillance, at a July 17, 2007 press conference to discuss the NIE, FBI Deputy Director John Pistole admitted the FBI was currently aware of no al Qaeda sleeper cells living inside the United States.<sup>24</sup>

## **DATA COLLECTION PROGRAMS CREATE SECURITY VULNERABILITIES**

Yet the greater concern is that these data collection programs will actually create new security vulnerabilities. On September 20, 2007, six technology experts from academia

---

<sup>18</sup> *Unlikely Terrorists on No-Fly list* (CBS News 60 Minutes television broadcast, October 8, 2006), available at <http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml> (updated June 7, 2007).

<sup>19</sup> Dep't. of Justice, Office of Inspector General, Follow-up Audit of the Terrorist Screening Center, (Sept. 2007), at iii, <http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf> [hereinafter TSC Audit Report]

<sup>20</sup> *Id.*

<sup>21</sup> Ellen Nakashima, *Terror Watchlist Yields few Arrests*, WASH. POST, Aug. 25, 2007, at A1, available at [http://www.washingtonpost.com/wp-dyn/content/article/2007/08/24/AR2007082402256.html?nav=rss\\_email/components](http://www.washingtonpost.com/wp-dyn/content/article/2007/08/24/AR2007082402256.html?nav=rss_email/components)

<sup>22</sup> Tom A. Peter, *National Intelligence Estimate: Al Qaeda stronger and a threat to US homeland*, CHRISTIAN SCIENCE MONITOR, July 19, 2007, <http://www.csmonitor.com/2007/0718/p99s01-duts.html>.

<sup>23</sup> TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, SYRACUSE UNIVERSITY, TRAC FBI REPORT: NATIONAL PROFILE AND ENFORCEMENT TRENDS OVER TIME (2006), <http://trac.syr.edu/tracfbi/newfindings/current/>.

<sup>24</sup> Michael Isikoff and Mark Hosenball, *The Flip Side of the NIE*, July 17, 2007, <http://www.msnbc.msn.com/id/19836407/site/newsweek/page/0/>.

and private industry released a comprehensive report detailing potential security hazards created by the PAA:

The Protect America Act, a law quickly proposed and enacted, potentially vastly increases the number of Americans whose communications and communication patterns will be studied. This sets up access to U.S. communications, a target of great value. The nation may build for its opponents something that would be too expensive for them to build for themselves: a system that allows them to see the intelligence interests of the U.S., a system that may tell them how to thwart those interests, and a system that might be turned to intercept the communications of American citizens and institutions.<sup>25</sup>

In addition to the technological vulnerabilities the PAA builds into the telecommunications system, these technology experts point to three serious security threats created when the government institutes mass data collection programs: “the danger that the system can be exploited by unauthorized users, the danger of criminal misuse by a trusted insider, and the danger of misuse by the U.S. government.”<sup>26</sup>

These threats speak directly to the concerns stated in the Chairmen’s letter regarding the potential breach of the increasing number of government databases containing American’s personal information, and the likelihood of this government using the data for purposes other than which it was originally collected.

## **1). POTENTIAL FOR MISUSE OF THE DATA COLLECTED**

The broad language contained in the PAA makes it likely that information collected under this authority will be used for purposes other than protecting and defending the national security. In fact, there is no requirement in the PAA that national security is even implicated before the NSA, a component of the Department of Defense, can begin spying on U.S. soil, potentially against U.S. persons and certainly against multi-national corporations that often possess detailed personal information about Americans. The PAA’s only requirement is that the DNI and Attorney General certify to themselves that a “significant purpose” of their surveillance is to obtain “foreign intelligence information,” and that the target of the surveillance is “reasonably believed” to be abroad (regardless of whether those targets are Americans, or are communicating with or about persons in the U.S.).

“Foreign intelligence information” is defined broadly in FISA to encompass any information that “relates to” the conduct of U.S. foreign affairs.<sup>27</sup> This could mean something as innocuous as an international business transaction or the travel plans of

---

<sup>25</sup> Steven Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford, “Risking Communications Security: Potential Hazards of the ‘Protect America Act,’” September 30, 2007, (on file with author), at 15.

<sup>26</sup> *Id.*

<sup>27</sup> 50 U.S.C. §1801(e)(2)(B).

American tourists. But more significant to the potential for misuse is the fact that the foreign intelligence collection does not have to be the only reason, or even the primary reason for the surveillance. The DNI and the AG are not even required to document the primary purpose of their surveillance, which means it would be difficult to determine why the information was originally collected. With no outside checks and balances there would be no way of knowing what information is being collected, why it is being collected, or how it is being used, so it would be virtually impossible to determine if the government was misusing information collected under the authorities granted in the PAA.

Moreover, the increased outsourcing of defense and intelligence functions to private companies means that for-profit enterprises are increasingly being given access to confidential government databases. For the companies involved, their partnerships with the government create unique business opportunities they can profit from, often at the expense of the privacy of the ordinary Americans who do business with them. It is impossible to know what these companies might do with the data they collect for the government, or with other information to which they have access to through their participation in these programs. Just as America Online (AOL) and Google routinely keep records of their customers' web searches to mine them for whatever business opportunities they might glean from the data, the private companies cooperating with government surveillance programs can also keep records of the requests the government makes to further plunder their customers' privacy for profit.<sup>28</sup> We can expect these companies to recognize that knowing what information the government is asking for will help them develop new products and services. These companies can then use this inside information to create new prediction tools to identify individuals that might later be of interest to counter-terrorism investigators. These new tools could then be marketed back to the government, or worse, to other clients, including private individuals, other commercial interests, and even foreign governments. The impact on the rights of Americans who are improperly identified as potential terrorists based on erroneous data or faulty prediction tools is immeasurable.

The PAA is not an isolated example. The government increasingly is ignoring the Congressional intent of the Privacy Act of 1974, enacted in the wake of the Nixon Presidency, in which government databases from the Internal Revenue Service and Social Security Administration were mined for data about President Nixon's perceived political enemies. The databases in question were collections of data about U.S. citizens' tax filings and retirement benefits earnings. In the last year, it has been revealed that a Department of Homeland Security Customs and Border Patrol program known as the Automated Targeting System (ATS), which was authorized by Congress to screen cargo entering the U.S. has been diverted to gather information on all travelers – including U.S. citizens – entering or exiting the U.S. and to assess whether they are a threat and assign

---

<sup>28</sup> See, Michael Barbaro and Tom Zeller, Jr., "A Face is Exposed for AOL Searcher No. 4417749," *New York Times*, Aug. 9, 2006, <http://www.nytimes.com/2006/08/09/technology/09aol.html?ex=1312776000&en=996f61c946da4d34&ei=5088&partner=rssnyt&emc=>

them a risk score.<sup>29</sup> Thus, the ATS data collection, which was created for one purpose has been entirely re-purposed – without Congressional authorization and in violation of the law – for another purpose.

## 2). RISK OF POTENTIAL BREACH OF GOVERNMENT DATABASES

Newly created intelligence databases will also be attractive targets for a host of enemies: identity thieves, malicious hackers, foreign companies eager to profit from industrial espionage, and most significantly, hostile foreign intelligence services. The collection of large volumes of sensitive information in the proliferating number of data warehouses would provide one-stop shopping for our adversaries because, as the Chairmen’s letter points out, our government has a dismal record of protecting sensitive information. And this problem is only compounded by the increased outsourcing of defense, intelligence and data processing functions to private companies who are not required to satisfy even basic data protection standards as a condition of their government contracts.

There are two separate avenues for breaching government databases. The first involves the misuse of the system by trusted insiders. The criminal convictions of long-time spies Aldrich Ames of the CIA and Robert Hanssen of the FBI, among others, demonstrate that individuals determined to betray our trust for private gain can defeat even the most stringent assessment programs of the most sophisticated intelligence agencies. That more agencies and even private contractors have access to sensitive databases today only increases the risk that someone could be persuaded to spy or be blackmailed into using their access for unlawful purposes. And it is not only intentional misconduct that can lead to the loss of sensitive data. Laptop computers, thumb drives and other data storage devices containing sensitive information can easily be lost, stolen, or misplaced. According to a 2007 Department of Justice IG’s audit, the FBI alone lost 160 laptop computers between 2002 and 2005, at least ten of which were determined to have contained sensitive or classified information.<sup>30</sup>

The second avenue for breaching government databases involves inappropriate access of unauthorized users. In 2005, Time Magazine reported a widespread Chinese cyber-espionage effort against U.S. intelligence targets federal investigators code-named “Titan Rain,” which penetrated computers at the U.S. Army Information Systems Engineering Command at Ft. Huachuca, Arizona, the Defense Information Systems Agency, the Naval Ocean Systems Center, the U.S. Army Space and Strategic Defense installation in Huntsville, Alabama in one twelve-hour period.<sup>31</sup> In 2006 a Romanian hacker was indicted for breaking into over 150 U.S. government computers, including “machines at NASA’s Jet Propulsion Laboratory and Goddard Space Flight Center, the Sandia National

---

<sup>29</sup> See, Sally B. Donnelly, “Airline ‘Risk Assessment’: Defending the Right to Snoop,” *Time Magazine*, Dec. 8, 2006, at: <http://www.time.com/time/nation/article/0,8599,1568354,00.html>.

<sup>30</sup> U.S. Department of Justice Inspector General, *The Federal Bureau of Investigation’s Control Over Weapons and Laptop Computers Follow-up Audit*, Audit Report 07-18, (Feb. 2007), at: <http://www.usdoj.gov/oig/reports/FBI/a0718/final.pdf>

<sup>31</sup> Nathan Thornburgh, “Inside the Chinese Hack Attack,” *Time Magazine*, Aug. 25, 2005, at: <http://www.time.com/time/nation/article/0,8599,1098371,00.html>



Laboratory, and the U.S. Naval Observatory.”<sup>32</sup> But this may be only the tip of the iceberg. Forbes Magazine reported that cyber-spies have also zeroed-in on softer targets - the private sector entities that have access to defense and intelligence information - including “the 10 most prominent U.S. defense contractors.”<sup>33</sup> The concern with these private entities is that they have a business interest in keeping quiet about such intrusions and data losses. Indeed, the FBI has reportedly launched an investigation against Unisys Corp., which had a \$1 billion dollar contract to build, secure and manage the information technology networks for the Transportation Security Administration and the Department of Homeland Security, for failing to detect and then covering-up computer intrusions of DHS systems by Chinese hackers.<sup>34</sup>

## CONCLUSION


The likelihood that these risks will become realized is increased under the PAA because it gives unchecked authority to an agency that has had very little oversight of any kind. This lack of oversight has produced predictable results. According to the *Baltimore Sun*, a 2007 NSA internal management study revealed that the agency “lacks vision and is unable to set objectives and meet them,” which mirrors the results of a similar study conducted in 1999.<sup>35</sup> That the NSA made no progress in correcting the deficiencies identified in the earlier study reveals the decay that comes from the lack of oversight. And this decay creates real security vulnerabilities, as mismanagement has been blamed for recent power outages at the NSA that have been predicted for a decade.<sup>36</sup>

The lack of judicial or congressional oversight of the authority granted in the PAA flies in the face of the careful framework of checks and balances built into our constitutional system of government. Clearly increased oversight would do more to protect our national security than granting the NSA unfettered authority to spy on Americans without sufficient cause.

Sincerely,



Caroline Fredrickson  
Director,  
Washington Legislative Office



Timothy Sparapani  
Senior Legislative Counsel



Mike German  
Policy Counsel

---

<sup>32</sup> Joris Evers, “Another Suspected NASA Hacker Indicted,” *CNET News*, Dec. 1, 2006, at: [http://www.news.com/Another-suspected-NASA-hacker-indicted/2100-7350\\_3-6140001.html](http://www.news.com/Another-suspected-NASA-hacker-indicted/2100-7350_3-6140001.html)

<sup>33</sup> Andy Greenberg, “Cyberspies Target Silent Victims,” *Forbes Magazine*, Sept. 11, 2007, at: [http://www.forbes.com/security/2007/09/11/cyberspies-raytheon-lockheed-tech-cx\\_ag\\_0911cyberspies.html](http://www.forbes.com/security/2007/09/11/cyberspies-raytheon-lockheed-tech-cx_ag_0911cyberspies.html)

<sup>34</sup> Ellen Nakashima and Brian Krebs, “Contractor Blamed in DHS Data Breaches,” *Washington Post*, Sept. 24, 2007, at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html>

<sup>35</sup> Siobhan Gorman, “Management Shortcomings Seen at the NSA,” *Baltimore Sun*, May 6, 2007, at: <http://www.baltimoresun.com/news/nation/bal-nsa050607.0.5435822.story>

<sup>36</sup> See Siobhan Gorman, “Power supply still a vexation for the NSA,” *Baltimore Sun*, June 24, 2007, at: <http://www.baltimoresun.com/news/nation/bal-nsa0624.0.5263352.story>