United States Senate
Select Committee on Intelligence
Hearing on the Patriot Act
April 19, 2005

Thank you, Mr. Chairman and members of the Committee. My name is Heather Mac Donald. I am a senior fellow at the Manhattan Institute for Policy Research, a think tank in New York City. I have written extensively on homeland security for the *Washington Post*, the *Wall Street Journal*, the *Los Angeles Times*, and *City Journal*, among other publications. I appreciate the opportunity to testify today on this important topic.

The most powerful weapon against terrorism is intelligence. The United States is too big a country to rely on physical barriers against attack; the most certain defense is advanced knowledge of terrorist plans.

In recognition of this fact, Congress amended existing surveillance powers after 9/11 to ready them for the terrorist challenge. The signal achievement of these amendments, known as the Patriot Act, was to tear down the regulatory "wall" that had prevented anti-terrorism intelligence agents and anti-terrorism criminal agents from sharing information. That wall was neither constitutionally nor statutorily mandated, but its effect was dire: it torpedoed what was probably the last chance to foil the 9/11 plot in August 2001. Thanks to the Patriot Act, all members of the anti-terrorism community can now collaborate to prevent the next terrorist strike before it happens.

Besides dismantling the wall, the Patriot Act made other necessary changes to surveillance law: it extended to terrorism investigators powers long enjoyed by criminal investigators, and it brought surveillance law into the 21st century of cell phones and e-mail. Where the act modestly expands the government's authority, it does so for one reason only: to make sure that the government can gather enough information to prevent terrorism, not just prosecute it after the fact.

Each modest expansion of government power in the Patriot Act is accompanied by the most effective restraint in our constitutional system: judicial review. The act carefully preserves the traditional checks and balances that safeguard civil liberties; four years after its enactment, after constant monitoring by the Justice Department's Inspector General and a host of hostile advocacy groups, not a single abuse of government power has been found or even alleged.

This record of restraint is not the picture of the act most often presented in the media or by government critics, however. The Patriot Act has been the target of the most successful disinformation campaign in recent memory. From the day of its passage, law enforcement critics have portrayed it as an unprecedented power grab by an administration intent on trampling civil rights.

As lie after lie accumulated, the administration failed utterly to respond. As a result, the public is wholly ignorant about what the law actually does. Hundreds of city councils have passed resolutions against the act; it is a safe bet that none of them know what is in it. The Committee is to be congratulated for taking the time to get the truth out.

Though the charges against the Patriot Act have been dazzling in their number, they boil down to four main strategies. This afternoon I would like to dissect those strategies, with particular reference to the most controversial sections of the act: sections 215 and 213. Discredit the anti-Patriot Act strategies in those contexts, and you have the key for discrediting them in every other context.

--Strategy #1: Hide the Judge.

The most pervasive tactic used against the Patriot Act is to conceal its judicial review provisions, as witnessed in the campaign against section 215. Section 215 allows anti-terror investigators access to business records in third party hands. The section may also be called the librarian's hysteria provision. The American Library Association has declared section 215 a

"present danger to the constitutional rights and privacy of library users," though the section says not a word about libraries. Such hyperbole is standard, and completely unwarranted.

The section works as follows: Under Section 215, the FBI may ask the Foreign Intelligence Surveillance Court for permission to seek business records—the enrollment application of a Saudi national in an American flight school, say—while investigating terrorism. The section broadens the categories of institutions whose records the government may seek, on the post-9/11 recognition that lawmakers cannot anticipate what sorts of organizations terrorists may exploit. In the past, to trace the steps of a Soviet spy, it may have been enough to get hotel bills or storage-locker contracts (two of the four categories of records covered in the previous section of the Foreign Intelligence Surveillance Act that Section 215 amended); today, however, gumshoes may find they need receipts from scuba-diving schools or farm-supply stores to piece together a plot to blow up the Golden Gate Bridge.

Section 215 removed the previous requirement in FISA that the records concern an "agent of a foreign power," since the scope of an anti-terror investigation is hard to predict in advance. An unwitting bystander may have purchased fertilizer for a terrorist posing as an aspiring farmer; finding out whether and how much fertilizer was purchased may be an essential link in the investigative chain.

These commonsensical reforms of existing investigative power have called forth a crescendo of hysteria. The ACLU warns that with section 215, "the FBI could spy on a person because they don't like the books she reads, or because they don't like the websites she visits. They could spy on her because she wrote a letter to the editor that criticized government policy." Librarians, certain that the section is all about them, are scaring library users with signs warning that the government may spy on their reading habits.

The force of these charges rests on the strategy of hiding the judge. Critics of section 215 conceal the fact that any request for items under the section requires judicial approval. An FBI agent cannot simply walk into a flight school or a library and demand records. The bureau must first convince the Foreign Intelligence Surveillance Court that the documents are relevant to protecting against international terrorism. The chance that the FISA court will approve a 215 order because the FBI "doesn't like the books [a person] reads . . . or because she wrote a letter to the editor that criticized government policy" is zero. If the bureau can show, on the other hand, that someone using a library's computers was seen with other terror suspects in Lahore, Pakistan, and has traveled regularly to Afghanistan under a false passport, then the court may well grant an order to get the library's Internet logs. As Andrew McCarthy has pointed out, literature evidence was a staple of terrorism prosecutions throughout the 1990's. Terrorists read bomb manuals, and often leave fingerprints on pages spelling out explosive recipes that match the forensics of particular bombings (like the 1993 attack on the World Trade Center).

Before the FBI can even approach the FISA court, agents must have gone through multiple levels of bureaucratic review just to open an anti-terror investigation. And to get to the court itself, intelligence agents must first persuade the Justice Department's Office of Intelligence and Policy Review that a section 215 order is warranted, a process of persuasion that traditionally has taken months of vetting and voluminous documentation.

--Strategy #2: Invent New Rights.

Besides concealing judicial review requirements, anti-Patriot Act demagogues also invent new rights. A running theme of the campaign against section 215 is that it violates the Fourth Amendment right to privacy. But there is no Fourth Amendment privacy right in records or other items disclosed to third parties. A credit-card user, for example, reveals his purchases to the seller and to the credit-card company. He therefore has no privacy expectations in the record of

those purchases that the Fourth Amendment would protect. As a result, the government, whether in a criminal case or a terror investigation, may seek his credit-card receipts without a warrant or "probable cause" to believe that a crime has been or is about to be committed.

Despite librarians' fervent belief to the contrary, this analysis applies equally to library patrons' book borrowing or Internet use. The government may obtain those records without violating anyone's Fourth Amendment rights, because the patron has already revealed his borrowing and web browsing to library staff, other readers (in the days of handwritten book checkout cards), and Internet service providers. It is worth noting, however, that after all the furor raised about library users' privacy rights, section 215 has not once been used to obtain library or book store records.

It is the lack of a Fourth Amendment privacy interest in third party records that has allowed prosecutors for decades to seek business and library records without any judicial review whatsoever. Section 215, by requiring judicial review, is far more protective of privacy than longstanding subpoena power in ordinary criminal investigations. Patriot critics have provided no evidence that the subpoena power has been abused to spy on Americans' reading habits; there is no reason to believe that section 215 will be any more susceptible to abuse.

Recipients of a section 215 production order may challenge the order in court, as Attorney General Alberto Gonzales recently testified, but they may not disclose the order in public. This is perfectly appropriate. Preemptive terror investigations cannot be conducted in the news media. The government would seek a terror suspect's airplane itineraries, for example, not in order to prosecute a hijacking after it happens, but to preempt a hijacking before the fact. The battleground is not the courtroom but the world beyond, where speed and secrecy can mean life or death.

--Strategy #3: Conceal Legal Precedent.

Attacks on the other most controversial section of the Patriot Act, section 213, illustrate the key ruse of concealing the act's legal precedents. Section 213 allows the government to delay notice of a search, something criminal investigators have been allowed to do for decades.

Say the FBI wants to plumb Mohammad Atta's hard drive for evidence of a nascent terror attack. If a federal agent shows up at his door and says: "Mr. Atta, we have a search warrant for your hard drive, which we suspect contains information about the structure and purpose of your cell," Atta will tell his cronies back in Hamburg and Afghanistan: "They're on to us; destroy your files — and the infidel who sold us out." The government's ability to plot out that branch of Al Qaeda is finished.

To avoid torpedoing preemptive investigations, Section 213 lets the government ask a judge for permission to delay notice of a search. The judge can grant the request only if he finds "reasonable cause" to believe that notice would result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or other serious jeopardy to an investigation. In the case of Mohammad Atta's hard drive, the judge will likely allow a delay, since notice could seriously jeopardize the investigation, and would likely result in evidence tampering or witness intimidation.

The government can delay notifying the subject only for a "reasonable" period of time; eventually officials must tell Atta that they inspected his hard drive.

Section 213 carefully balances traditional expectations of notice and the imperatives of preemptive terror and crime investigations. That's not how left- and right-wing libertarians have portrayed it, however. They present Section 213, which they have dubbed "sneak-and-peek," as one of the most outrageous new powers seized by former Attorney General John Ashcroft. The ACLU's fund-raising pitches warn: "Now, the government can secretly enter your home while you're away . . . rifle through your personal belongings . . . download your computer files . . .

and seize any items at will. . . . And, because of the Patriot Act, you may never know what the government has done."

Notice the ACLU's "Now." Like every anti-213 crusader, the ACLU implies that section 213 is a radical new power. This charge is a rank fabrication. For decades, federal courts have allowed investigators to delay notice of a search in drug cases, organized crime, and child pornography, for the same reasons as in section 213. Indeed, the ability to delay notice of a search is an almost inevitable concomitant of investigations that seek to stop a crime before it happens. But the lack of precise uniformity in the court rulings on delayed notice slowed down complex national terror cases. Section 213 codified existing case law under a single national standard to streamline detective work; it did not create new authority regarding searches. Those critics who believe that the target of a search should always be notified prior to the search, regardless of the risks, should have raised their complaints decades ago--to the Supreme Court and the many other courts who have recognized the necessity of a delay option.

Critics of Section 213 raise the spectre of widespread surveillance abuse should the government be allowed to delay notice. FBI agents will be rummaging around the effects of law-abiding citizens on mere whim, even stealing from them, allege the anti-Patriot propagandists. But the government has had the delayed notice power for decades, and the anti-Patriot demagogues have not brought forward a single case of abuse under delayed notice case law. Their argument against Section 213 remains purely speculative: It *could* be abused. But there's no need to speculate; the historical record refutes the claim.

Moreover, such wild charges against Section 213 "hide the judge." It is a federal judge who decides whether a delay is reasonable, not law enforcement officials. And before a government agent can even seek to delay notice of a search, he must already have proven to a judge that he has probable cause to conduct the search in the first place. This is hardly a recipe

for lawless executive behavior—unless the anti-Patriot forces are also alleging that the federal judiciary is determined to violate citizens rights. If that's what they mean, they should come out and say it.

In fact, the recent history of government intelligence-gathering belies the notion that any government surveillance power sets us on a slippery slope to tyranny. There *is* a slippery-slope problem in terror investigations — but it runs the other way. Since the 1970s, libertarians of all political stripes have piled restriction after restriction on intelligence-gathering, even preventing two anti-terror FBI agents in the same office from collaborating on a case if one was an "intelligence" investigator and the other a "criminal" investigator. By the late '90s, the bureau worried more about avoiding a pseudo-civil liberties scandal than about preventing a terror attack. No one demanding the ever-more Byzantine protections against hypothetical abuse asked whether they were exacting a cost in public safety. We know now that they were.

The libertarian certainty about looming government abuse is a healthy instinct; it animates the Constitution. But critics of the Patriot Act and other anti-terror authorities ignore the sea change in law enforcement culture over the last several decades. For privacy fanatics, it's always 1968, when J. Edgar Hoover's FBI was voraciously surveilling political activists with no check on its power. That FBI is dead and gone. In its place arose a risk-averse and overwhelmingly law-abiding Bureau, that has internalized the norms of restraint and respect for privacy.

This respect for the law now characterizes intelligence agencies across the board. Lieutenant General Michael V. Hayden, the nominee for Principal Deputy Director of National Intelligence, told this committee last week that the challenge for supervisors in the National Security Agency was persuading analysts to use all of their legal powers, not to pull analysts back from an abuse of those powers.

It is because of this sea-change in law enforcement culture that Patriot Act critics cannot point to a single abuse of the act over the last four years, and why they are always left to argue in the hypothetical.

--Strategy #4: Reject Secrecy.

A subtext of many Patriot Act critiques is a refusal to grant any legitimacy to government secrecy. Recipients of document production orders in terror investigations—whether Section 215 orders or national security letters under the 1986 Electronic Communications Privacy Act--should be able to publicize the government's request, say the critics; targets of searches should be notified at the time of the search. Time and again, law enforcement critics disparage the Foreign Intelligence Surveillance Court, because its proceedings are closed to the public. The ACLU, for example, opposes the roving wiretap authority for terrorism investigations in the Patriot Act (Section 206), even though criminal investigators have long had the roving wiretap option, because Section 206 wiretaps "are authorized secretly without a showing of probable cause of crime." (Section 206 requests must demonstrate probable cause that the wiretap target is an agent of a foreign power and that he will be using the tapped communications devices.)

This transparent approach may satisfy those on the left and right who believe that the American people have no greater enemy than their own government, but it fails to answer the major question: how would it possibly be effective in protecting the country? The Patriot Act critics fail to grasp the distinction between the prosecution of an already committed crime, for which probable cause and publicity requirements were crafted, and the effort to preempt a catastrophic attack on American soil before it happens. For preemptive investigations, secrecy is of the essence. Opponents of the Patriot Act have never explained how they think the government can track down the web of Islamist activity in public.

These four strategies, in various combinations—hide the judge, invent new rights, conceal legal precedent, and reject secrecy—lie behind nearly all of the Patriot Act attacks. The crusade against Section 214, for example, which allows the government to record the numbers dialed from a phone if relevant to a terrorism investigation (the so-called pen register power), uses all four strategies. (A related section, Section 216, extends the longstanding rules on pen registers, to the 21st century technologies of e-mail. Section 216 allows the government to capture only an e-mail's routing and addressing information, not its content.)

Section 214 merely allows the agents investigating a terrorism case the same power that criminal investigators have. But the Electronic Frontier Foundation calls the section "a serious threat to privacy." This charge rests on inventing new rights. In fact, pen registers threaten no privacy rigths, as the Supreme Court has held, because there is no legitimate expectation of privacy in the numbers dialed from a phone, which are recorded already by telephone companies. Even though judicial authorization for a pen register is not constitutionally required, section 214 nevertheless mandates that the government obtain an order from the FISA court for their use. EFF dismisses the value of the court, however, because it "operates in total secrecy."

In conclusion, the Patriot Act is a balanced updating of surveillance authority in light of the new reality of catastrophic terrorism. It corrects anachronisms in law enforcement powers, whereby health care fraud investigators, for example, enjoyed greater ability to gather evidence than Al Qaeda intelligence squads. It created no novel powers, but built on existing authorities within the context of constitutional checks and balances. It protects civil liberties while making sure that intelligence analysts can get the information they need to protect the country. The law should be reenacted.