Bill as Introduced

HCR 9 - AS INTRODUCED

2003 SESSION

03-0710
05/09

HOUSE CONCURRENT RESOLUTION *9*

A RESOLUTION urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

SPONSORS: Rep. Almy, Graf 18; Rep. Kurk, Hills 48; Rep. M. Smith, Straf 72; Rep. Buhlman, Hills 66

COMMITTEE: State-Federal Relations and Veterans Affairs

ANALYSIS

This resolution urges the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

HCR 9 – AS INTRODUCED

03-0710
05/09

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Three

A RESOLUTION urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

Whereas, our nation and our state were founded to escape and prevent tyranny by the establishment of multiple checks upon the power of our respective governments, and by the careful restraint of our military's power over our civilian population; and

Whereas, the Department of Defense of the United States of America is now exploring a program named Total Information Awareness which would attempt to requisition and correlate every existing private and public database on our nation's individual citizens and residents; and

Whereas, these databases are said to include those of credit records, employment histories, gun registries, medical records, educational records, drivers' licenses, catalog purchases, civil lawsuits, criminal proceedings, Social Security information, professional licenses, passport applications, civil and military service dossiers, bank accounts, computerized road toll records, IRS records, insurance records, savings and debt transactions, airline travel, FBI and police dossiers, video and cable viewing records, surveillance cameras, computer activity records, and library records; and

Whereas, this degree of government knowledge of the lives of ordinary Americans, and potential control of their individual data, could be devastating to our liberty and our republic, if ever used for personal or political gain by individual government employees, or by a future commander in chief or agency head for control of legitimate domestic dissent, political activity, key economic actors, or the media; and

Whereas, even under the assumption that no future office-holder would be tempted by the illegitimate abuse of this vast power over the citizenry, the temptation to extend its use into the civilian concerns of ordinary crime would be difficult to resist and effectively abolish all constitutional guarantees against government searches and seizures; now, therefore, be it

Resolved by the House of Representatives, the Senate concurring:

That the Commander in Chief and the Joint Chiefs of Staff of the United States of America are strongly urged to abandon the attempt to implement the Total Information Awareness program; and

That copies of this resolution be forwarded by the house clerk to each member of the New Hampshire congressional delegation, the President of the United States, and the Joint Chiefs of Staff in Arlington, Virginia.

Amendments

Rep. Almy, Graf 18
Rep. Kurk, Hills 48
Rep. Hatch, Carr 7
Rep. Buhlman, Hills 66
May 6, 2003
2003-1515h
05/01

Amendment to HCR 9

Amend the resolution by replacing the title of the resolution with the following:

A RESOLUTION urging the United States Congress to ensure the constitutionality of the implementation of the Total Information Awareness Program, the USA PATRIOT ACT, and any successors.

Amend the resolution by replacing all after the title with the following:

Whereas, our nation and our state were founded to escape and prevent tyranny by the establishment of multiple checks upon the power of our respective governments, and by the careful restraint of executive and military power over our civilian population; and

Whereas, the Department of Defense of the United States of America has been exploring a program named Total Information Awareness which would attempt to requisition and correlate every existing private and public database on our nation's individual citizens and residents; and

Whereas, these databases are said to include those of credit records, employment histories, gun registries, divorce, medical, and educational records, drivers' licenses, catalog purchases, civil lawsuits, criminal proceedings, Social Security information, professional licenses, passport applications, civil and military service dossiers, bank accounts, computerized road toll records, IRS records, insurance records, savings and debt transactions, airline travel, FBI and police dossiers, video and cable viewing records, surveillance cameras, computer activity records, and library records; and

Whereas, this degree of government knowledge of the lives of ordinary Americans, and potential control of their individual data, could be devastating to our liberty and our Republic, if ever used for personal or political gain by individual government employees, or by a future Commander in Chief or agency head for control of legitimate domestic dissent, political activity, key economic actors or the media; and

Whereas, even under the assumption that no future office-holder would be tempted by the illegitimate abuse of this vast power over the citizenry, the temptation to extend its use into the civilian concerns of ordinary crime would be difficult to resist, and effectively abolish all Constitutional guarantees against government searches and seizures; and

Whereas, the United States Congress has recently established budgetary controls to require strict accounting from the Department of Defense of constitutional and legal privacy concerns before the Total Information Awareness program is allowed to proceed; but

Whereas, on October 24, 2001, in the shadow of the atrocious acts occurring on September 11, 2001, the United States Congress, before applying its usual careful consideration, passed the USA PATRIOT ACT, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; and

Whereas, this act has made it legal for government agents to enter and search a citizen's home, or obtain an individual's or a class of citizens' medical, bank, credit, business, library, and other records, using a warrant issued by a secret court that is barred by the act from refusing the government's request, and withholding from those citizens and the public the knowledge that the search and seizures have occurred; and

Whereas, these powers can be used in investigations having nothing to do with terrorism, requiring only an agent's allegation that the investigation may touch on terrorism; and

Whereas, the existing war on terrorism is not a war in the traditional sense of the term, but a state of alertness without an end limit, and therefore could be used to justify the permanent destruction of our cherished liberties and way of life unless appropriate action is taken; and

Whereas, the USA PATRIOT ACT defines the new crime of domestic terrorism in such a way that many ~~if not most~~ advocacy groups in this nation could qualify as terrorist, if the Attorney General of the United States so chooses; and

Whereas, the government is reportedly ~~planning~~ considering an expansion of these powers, called the Domestic Security Enhancement Act of 2003, which defines domestic crimes for which an American citizen could be stripped of citizenship; and

Whereas, the Attorney General is granted the power to remove many of the checks and balances that have preserved our liberty and our security for more than 220 years, and particularly those of judicial and public scrutiny; now, therefore, be it

Resolved by the New Hampshire House of Representatives, the Senate concurring:

That the Congress of the United States of America is to be commended for its actions to date in protecting our cherished liberties relative to the Total Information Awareness program; and

That the United States Congress is strongly urged to undertake an investigation of the USA PATRIOT ACT to determine how it has been used, and to repeal or amend any provisions that have resulted in undue infringements on the legal activities of the citizens and residents of this great country, thereby restoring confidence in the protections guaranteed under the Bill of Rights; and

That the United States Congress is urged to prevent the further expansion of these intrusive government powers by refusing to consider the Domestic Security Enhancement Act unless it is amended to respect all the guarantees of the Bill of Rights; and

That copies of this resolution be forwarded by the house clerk to the President of the United States, the Attorney General, the Joint Chiefs of Staff in Arlington, Virginia, and each member of the New Hampshire congressional delegation.

2003-1515h

AMENDED ANALYSIS

This resolution urges the United States Congress to ensure the constitutionality of the implementations of the Total Information Awareness Program, the USA PATRIOT ACT, and any successors.

Committee Minutes

Date: May 7, 2003
Time: 3:40 p.m.
Room: LOB, Room 101

The Senate Committee on Interstate Cooperation held a hearing on the following:

HCR 9 urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

Members of Committee present: Senator Gatsas
Senator Estabrook
Senator Clegg

The Chair, Senator Theodore Gatsas, opened the hearing on HCR 9 and called on the prime sponsor, Representative Almy, to introduce the bill.

Representative Susan Almy: Thank you, Mr. Chairman. Mr. Chairman and members of the Committee, I'm Representative Susan Almy, House District 18. That's Lebanon, Grafton County.

On September 11 of 2001, this nation had a major shock. While we were still suffering from this shock, John Ashcroft brought the USA Patriot Act to the U.S. Congress for passage. Never heard or read in the House and only read in the Senate after passage, it provided tools that our nation needed to fight back against the shadowy enemy. But, it was passed virtually without deliberation and many members of Congress are now realizing that they went too far and sacrificed part of the essential spirit of this country.

I spent many years overseas learning what is special about our country – freedom of expression, freedom to assemble, freedom from being dogged by government spies anywhere you go to make sure you toe the government line.

Other sponsors of the amendment that we are bringing you, and its previous incarnations, cover the gamut of political activity in this State and experience in and out of the executive government and of the military. But, in this we are acting as citizens, not as politicians. We wish to send a message to

Congress to help them to have the political will to re-examine what they passed in the USA Patriot Act and to resist the unconstitutional aspects of the successor bill that is now being brought forward.

This bill began as a resolution against the most immediate threat related to the Patriot Act, which was the Pentagon's Total Information Awareness Program. The Total Information Awareness Program intended to correlate every public and non-public database in the country and look for patterns that might indicate a terrorist at work. Things like anyone who bought fertilizer and rented a truck in the same week. There would have been a lot of false positives. They didn't know if they had the technology to do it, so they wanted to try it first and answer questions later.

When columnist William Safire blew the whistle on it last November, leading to immense outrage around the country, the U.S. Senate passed the Widen Amendment to the budget in January denying the program funding until the Pentagon could explain how it could be implemented without violating the Constitution and the existing privacy laws of this nation. The U.S. House concurred and it is now law.

But, if the Congress wants to be clear about it's message, it needs to re-examine parts of the USA Patriot Act that violate American citizens' rights to protection from warrantless search and seizure, to freedom of assembly and speech.

Our group of sponsors asked the New Hampshire House to pass a resolution against the Total Information Awareness Program and they have sent this on to you. We are now asking you to adopt the amendment that speaks to the broader rights denied to New Hampshire citizens by the USA Patriot Act as well.

I provided a lot of materials. I just wanted to go through them very briefly. Safire's column, a summary from the Electronic Privacy Information Center, an editorial from the Cato Institute, and a small piece from the *Boston Globe* talking about the Widen amendment which is attached onto a piece from the internet with the first part of the amendment on it. Then there are materials on the USA Patriot Act, which Representative Smith is going to talk about and we are hoping that Representative Kurk is going to get away from wherever he has been caught. The other sponsors are all doing other bills. The materials on the USA Patriot Act, including Cato Institute article again explaining the USA Patriot Act's attacks on civil liberties. Eight separate sections from that Act and a discussion from the FindLaw website of the follow-up legislation to the Patriot that the Department of Justice is planning to propose to Congress. There is also a copy of a resolution that passed the

New Mexico House, which is much stronger than we wanted to be at this point about the Patriot Act. I have provided for the Committee a very detailed two-part article that I thought most people would want to wade through on how the Patriot Act is being used a year later, which comes from the website. **(Please see attachments.)**

I wanted to close my piece of this by saying that the USA Patriot Act puts us on a war footing, but terrorism is not a war; terrorism never ends. I have lived in many countries where terrorism is a fact of life and it does not go away. We may gradually, over the years, become used to it, but it does not go away. We must learn to adapt the methods of fighting it to our ...(inaudible)... if we want to remain the nation that we are.

Senator Theodore L. Gatsas, D. 16: Are there any questions?

Senator Robert Clegg, Jr., D. 14: I have just one. Why is it that you didn't try to get this amendment through in the House?

Representative Almy: We did not put it, we were trying to put it in to the Committee at the time that they passed it. They told us that they would retain the bill and we thought we would have a couple of months to think about it and make it stronger. Then we found out that they just passed the bill and we had not yet been back to them to tell them that the U.S. Senate had already put this in the budget for the Total Information Awareness Act. So, they were unaware that this did not need to go forward very quickly.

Senator Robert Clegg, Jr., D. 14: It sounded like this bill must have gone through the Finance Committee?

Representative Almy: No, actually. I admit...

Transcriber's note: laughter and comments among Senators and audience, much too jumbled for transcription.

Representative Almy: There seems to be some very strong relationships, at least in the House, between financial, fiscal, integrity and some of these other concerns. I found that also in the Ways and Means Committee.

Senator Robert Clegg, Jr., D. 14: Thank you. I had to take my shot at the House.

Senator Iris Estabrook, D. 21: Are there further questions?

Representative Almy: Would you like me to repeat the opening?

Senator Iris Estabrook, D. 21: No. I don't. Thank you for your testimony. Representative Kurk?

Representative Neal Kurk: Thank you, Madam Chairman. Good afternoon to you and members of the Committee. For the record, my name is Neal Kurk, representing Hillsborough District 48, the towns of Goffstown and Weare.

Senator Clegg, I think there was another reason why the amendment was not presented to the House and was not part of the original bill. We were focusing on what were considered to be emergency needs. The Total Information Awareness Program was going into effect. We wanted to focus on that immediately and therefore decided that these other issues were not as paramount and we didn't want to complicate the bill with these other issues. It turned out, as Representative Almy said, the U.S. Senate made the determination that the Total Information Awareness Program needed to have a time out and they took care of that problem. Hence, we went back to the Committee and this all happened while the bill was going through the process. Hence, we went back to the Committee, as Representative Almy said, to try to make a change and, as it turned out, it was too late, and therefore, we are bringing it forward in the Senate as the next opportune time.

This bill is an attempt to balance our need for protection against terrorism and protection for our personal safety against our need for constitutional liberties. This HCR, in effect, wants to make sure that the Bill of Rights still reigns paramount in the United States. The USA Patriot Act and the proposed amendments to it basically go too far in redressing the balance between safety and liberty. This bill, very simply says, no, you have gone too far. If we have to give up our liberties for safety, the terrorists have won. We don't want to do that. We think there are other better ways to do it. The idea that the government can secretly, without showing probable cause, but alleging some connection with terrorism, go into your home and put a key tap on your computer or take or copy any computer records and you'll never know about that I find shocking. It's not something that I could even dream could occur in the United States. If George Orwell wrote about it, I might be able to enjoy it in a moment of science fiction, but that is about as far.

Apparently, people have become so obsessed with safety that they are willing to give up liberty for this. I think, in New Hampshire, we feel differently and I would hope that the Senate would concur with that and pass this resolution.

Thank you, Madam Chair.

Senator Iris Estabrook, D. 21: Thank you for your testimony. Questions?

Senator Robert Clegg, Jr., D. 14: Neal, lines 18 and 19 in the amendment. I know what you are trying to do. You and I have worked on privacy before, but I am not comfortable making a statement that says many if not most advocacy groups in this nation would qualify as terrorists unless you have something that you can show me in the law that...

Representative Kurk: Am I reading something different?

Senator Robert Clegg, Jr., D. 14: Page 2. Sorry. My fault.

Representative Kurk: If you wanted to eliminate that, it wouldn't bother me because I don't have any backup for that, although I'm told that the ACLU...

Senator Robert Clegg, Jr., D. 14: The other thing is, on line 21, the government is reportedly. I'm not comfortable with that language either.

Representative Kurk: I don't know if it has been introduced, but a bill is being drafted now and it has been reported in the newspapers and you see the title here. That doesn't mean that it will be...

Senator Robert Clegg, Jr., D. 14: I think Dick Green stated it best when he said "I don't believe anything I read in the newspaper even though I know half of it to be true".

Unidentified speaker: What line are you on?

Senator Robert Clegg, Jr., D. 14: I'm sorry. Line 21 on page 2.

Senator Iris Estabrook, D. 21: I would like to follow up that question. Do you think we could just change whatever you are planning to considering and you wouldn't have a true statement?

Representative Kurk: Yes.

Senator Iris Estabrook, D. 21: Further questions? Thank you very much.

Representative Kurk: I must say, Senator Clegg, that I'm delighted to notice that you have retained some of your habits as House member and you are actually reading these things, maybe simultaneously, but at least you're reading them. Thank you.

Senator Robert Clegg, Jr., D. 14: That's because I didn't take reading recovery.

Representative Kurk: I'm pushing early literacy, not reading recovery, but nice try.

Senator Iris Estabrook, D. 21: Did you go to preschool?

Senator Robert Clegg, Jr., D. 14: I never went to school, come to think of it.

Senator Iris Estabrook, D. 21: Any school. Thank you. Welcome Representative Smith.

Representative Marjorie Smith: Thank you. I didn't wait to be asked. I'm sorry.

Senator Iris Estabrook, D. 21: That's alright. You were clearly next.

Representative Smith: Representative Marjorie Smith from Strafford 72, I believe that is Durham, Lee and Madbury.

I don't want to belabor this. I think that both Susan and Neal were quite eloquent, but I do want to address Senator Clegg's civic question.

Section 802 of the federal defines domestic terrorism and it says, activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States that appear to be intended to intimidate or coerce civilians, to influence the policy of government to effect the conduct of the government by mass destruction, assassination or kidnapping. The others, obviously, were much more mild. And that occur primarily within the territorial jurisdiction of the states.

Well, you know, none of us thinks terrorists are terrific and don't want them in our neighborhood, but if you read the definition, if you or your legal partner, because of course, we are our brother's keepers under this, send dues to an organization that the government might consider suspect, you are liable to be accused of being a terrorist. Let me give you examples of organizations that conform with this definition. Green Peace, which tries to interfere with acts that they believe are harmful. The organization that exists for the effective treatment of animals, which takes sometimes very strong stands against animal experimentation. The tree sitters in the Northwest trying to protect the sequoias. Operation Rescue, which tries to interfere with women who have chosen to approach a clinic possibly for an abortion. Motorcycle groups, which are viewed to be threatening to people. Militias or any public

demonstration during which a few troublemakers set off activities that require coercive or active police response. I actually read this twice because I thought, "Oh my, we are going to get the UNH students" under this.

Senator Iris Estabrook, D. 21: Hockey night.

Senator Robert Clegg, Jr., D. 14: No, I think you just described the Legislature.

Representative Smith: Strikes, which interfere with the normal course of a particular business. These definitions are so shockingly broad and vague that no one is protected and we all like to think that this won't happen to us because we are law abiding, we are honest, we are legislators. But in fact it can happen in the most innocuous way and there are no protections. I have page after page where I can give you those kinds of examples and I don't want to belabor it. I know we have been all day and we are tired. But, disclosure of educational records. No right to any privacy. The use of pen registers and something called track and trace devices. I don't think that has to do with little Adam who was running around, but it is a way to capture electronic signals that come from, whether it is your telephone or your computer or whatever. It is page after page after page of this.

I think that one of the things that is most interesting about us doing this is that it will not fall on deaf ears. I believe that there are increasing numbers of members of the United States Congress who have come, are beginning to feel some real concerns about what they did. The situation we explained to you about Total Information Awareness, which was going out of the Defense Department under the jurisdiction of John Poindexter, caused so many people to be frightened and the Congress to be frightened, that they said wait a minute, t for time out. And they stopped that. They are now beginning to look at this and I think it does nothing but help to add to this community of concern to cause people to take a look and say, "What is responsible here and what is not and what do we give up?"

If we give up our liberty, to have security, we might as well all pack our bags. So, there are very specific examples. This is not a question of theoretically saying that at some difficult to imagine circumstance there might be negative impacts on the citizens of this state. This is real and we think it is time to add our voices to those voices across the country and say this is not the country that we want to live in.

Senator Iris Estabrook, D. 21: Thank you. Questions?

Senator Robert Clegg, Jr., D. 14: I notice you have notes on that. Can we get a copy of that for the Committee so that...

Representative Smith: Of course. I'm happy to.

Representative Almy: You have that in your packet.

Senator Robert Clegg, Jr., D. 14: I do in the packet that you gave out?

Representative Almy: I think it is.

Senator Robert Clegg, Jr., D. 14: Mine is newspaper articles. Yes, I do have it. Thank you.

Representative Smith: I can give you another copy, but I think it's silly to do that unless you want more information. Thank you very much.

Senator Iris Estabrook, D. 21: Any further questions?

Senator Robert Clegg, Jr., D. 14: No, I'm all set.

Senator Iris Estabrook, D. 21: Thank you very much.

Representative Smith: Thank you, Madam Chair. Senator Martel said you do a very nice job.

Senator Iris Estabrook, D. 21: It's my five minutes of chairdom. Claire Ebel? Welcome to the Committee.

Claire Ebel: Thank you. My name is Claire Ebel. I am Executive Director of New Hampshire Civil Liberties Union and, unlike Representative Smith, I do intend to belabor this point. My job here is to scare the living whatever out of you and I hope, in a few minutes, I can do exactly that.

Several years ago, 1989 to be exact, Representative Kurk, among others, sponsored 201-B:11, which is the library user reference confidentiality provision in our state statutes. It was a result of what happened to Justice Bourque when he was nominated to the Supreme Court or when it was announced that he was to be nominated. They started rummaging through his library records, his video rentals, etc., trashing the man's privacy among other things. Representative Kurk submitted and shepherded through the Legislature this bill which protects our privacy.

Silly us because we didn't know about a provision in the USA Patriot Act that would come along fourteen years later. It is called safe harbor and I know you had that in a bill before. This is a different kind of harbor. Notwithstanding any other provision of this title, any consumer reporting agency or agent or employee (this is specific to that area) relying on a good faith reliance or upon a certification of a governmental agency pursuant to the provisions of this section (I'd love to know who wrote this) shall not be liable to any person for disclosure under this subchapter. Shall not be liable under the Constitution of any state or liable under any law or regulation of any state or any political subdivision of any state. In other words, in this section of the USA Patriot Act, the Constitution and the state statutes of New Hampshire be damned. The USA Patriot Act prevails.

Representative Smith mentioned to you and, Senator Clegg, I would suggest that on page 2, line 19, you strike the words "if not most". So, it would read "Whereas, the USA Patriot Act defines the new crime of domestic terrorism in such a way that many advocacy groups...could qualify as terrorist..." I think it is an overstatement to say "if not most".

But, let me give you some other concrete examples. My son is now almost a twenty-five year old law student in environmental law. When he was a little boy, I used to send money for him in lieu of part of his Christmas gift to groups of his choosing and he loved whales and marine biology and so, from the time he was four years old, I was sending money to different groups. We adopted a whale one year. It was our whale along with, I'm sure, three or four million other people, but Brian thought it was his. One of the groups we sent money to was the Sea Shepherd Society. Now, you may remember that group by its actions and not by its name. They were the people who put their boats between the whalers and the whales. Were they breaking the law? You bet. Were they endangering life, very possibly their own or someone on the whaling ship when they attempted to coerce the government and intimidate governments to change their policies? You bet. That was twenty years ago. But the fact that twenty years ago I made that contribution could now put me in a position of being declared a terrorist if Attorney General Ashcroft tomorrow or next week or next year decides that the Sea Shepherd Society is a terrorist organization. They certainly fit the definition.

Another group that clearly fits the definition is the WTO protesters, who did everything to try to coerce and intimidate during the protest, who did clearly cause injuries and endanger human life and the fact is, their actions were not legal. We can constitute them now, under existing statutes, for breaking the laws, but to declare them terrorists is to raise the bar so high as to stifle their legitimate First Amendment activity, their rights to speak and their rights to protest.

Representative Smith also made reference to Section 802, I mean, I beg your pardon, Section 508, which deals with educational information. There is a very perverse part of the provision that opens up the National Education Statistics Act of 1994 in the USA Patriot Act. Those are very personal, private, intimate statistics that are gathered from every student who wants to get federal assistance - Stafford loans, Pell grants, whatever. The data is collected on the guarantee by the government in writing on the form that these forms are for statistical purposes only, that individual information will never be released, that it will only be aggregated and published in the aggregate. USA Patriot Act says tough grubbies. We are going to get the individual statistics, we are going to examine them, and we may, in fact, detain or interrogate individuals based on information that the United States government told them would never be released. USA Patriot releases.

There is a section called Section 215 in the USA Patriot Act that basically says to you, if you have ever had an abortion, we can find out. If you have ever been treated for depression, we can find out. If you have ever been treated for a venereal disease, we'll know. If you have ever inherited money and spent it on gambling, we're going to find out. If you have engaged in activities which may not show up on a police blotter because you were not convicted, we will know. If you have engaged in activities that you may not want the government to know, we will know. They can get your library records, your financial records, your medical records, your educational information, every shred of data that exists anywhere in this country on you, they can get, they can compile and then they can take action against you if they decide there is something about you that they want to learn more about. That was the kind of trace and pen register and trap and trace device that Representative Smith referred to. That particularly is a perverse section of this law.

Under Section 216... This law is supposedly, and I actually clipped the title because I would like to find out someday how much they paid to the person who came up with USA Patriot. It's a word like scuba. It stands for Uniting and Strengthening America by Providing Appropriate...

Tape change.

Ms. Ebel: Tools Required to Intercept and Obstruct Terrorism. USA Patriot.

In Section 216, the search powers that they talk about throughout this bill that have to have some relationship to terrorism are set aside and Section 216 says, "upon an application made under this section, the court shall enter an ex parte order". There is no court review in any part of the USA Patriot

Act. The justices are required to grant the warrant or the ability if anyone asserts what they are looking for. The authorization for a pen register or trap and trace device within the jurisdiction, if the court finds that the state law enforcement, the state law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. This gives state law enforcement the right to tap your phone, to listen in to your phone calls, regardless of where you made them, to tap your computer and follow the trail of your e-mails without a warrant, only on an assertion that they think they are going to get what they are looking for and the judge has no power to review their evidence and say, "I don't think so. You're not getting a warrant on this basis". This extends the ability to act without a warrant, to local law enforcement in terms of investigations of criminal activity having nothing to do with terrorism.

This bill, when it was voted overwhelmingly by the United States Congress, Representative Almy alluded to the fact, but I think it bears repeating, nobody had read it. They took the assertions of Attorney General Ashcroft and others what was in the bill and it is not clear, Irish person that she is, exaggerating, as she often does. This bill wasn't even printed when it was passed. Nobody could have read it. They didn't have it in their hands.

I would urge you to amend HCR 9 to include, not a repeal of the USA Patriot Act, which is what I would like, but simply an investigation of whether or not we are living the quote that Benjamin Franklin made two hundred and seventeen years ago. "He who would give up essential liberty for a little temporary safety deserves neither liberty nor safety". To that, my personal hero, Thomas Jefferson, added, "And he will lose both".

And, I have copies of the sections of the bill that I will give to you, Senator. And, I made copies of two articles that appeared in yesterday's *Monitor*. One was the release of twenty-two prisoners from Quantanomo, one of them as young as thirteen years of age. Part of the USA Patriot Act is detention. One is something that I am probably the only one in the room old enough to remember. It was a release of the transcripts from what we called when I was a kid, "The Army McCarthy hearings" and I think it is very relevant.

I'm sorry to speak so long. This is something that you might have gathered that I am very passionate about.

Senator Iris Estabrook, D. 21: Thank you very much. Questions?

Ms. Ebel: Senator Clegg doesn't have a question?

Senator Iris Estabrook, D. 21: No questions. Sorry to disappoint.

Senator Robert Clegg, Jr., D. 14: I'm afraid that I would agree with her in public and that would be the second time this year.

Claire Ebel: Senator, I will leave the room.

Senator Iris Estabrook, D. 21: Can't have that on the record.

Senator Robert Clegg, Jr., D. 14: Right, can't have that on the record.

Senator Iris Estabrook, D. 21: Thank you very much. Is there anyone else who would like to testify on HCR 9? Seeing none, I will close the hearing on HCR 9 and thank you all very much.

Hearing concluded at 4:10 p.m.

Respectfully submitted,

L. Gail Brown
Senate Secretary
6/12/03

ELECTRONIC PRIVACY INFORMATION CENTER

Total Information Awareness (TIA)

Introduction | News | Resources

Introduction

The Total Information Awareness project is part of the Defense Advanced Research Projects Agency's Information Awareness Office. The office is headed by Admiral (retired) John Poindexter who is responsible for conceiving the project. TIA purports to capture the "information signature" of people so that the government can track potential terrorists and criminals involved in "low-intensity/low-density" forms of warfare and crime. The goal is to track individuals through collecting as much information about them as possible and using computer algorithms and human analysis to detect potential activity.

The project calls for the development of "revolutionary technology for ultra-large all-source information repositories," which would contain information from multiple sources to create a "virtual, centralized, grand database." This database would be populated by transaction data contained in current databases such as financial records, medical records, communication records, and travel records as well as new sources of information. Also fed into the database would be intelligence data.

A key component of the TIA project is to develop data-mining or knowledge discovery tools that will sort through the massive amounts of information to find patterns and associations. TIA will also develop search tools such as Project Genoa, which Admiral Poindexter's former employer Syntek Technologies, assisted in developing. TIA aims to fund the development of more such tools and data-mining technology to help analysts understand and even "preempt" future action.

A further crucial component is the development of biometric technology to enable the identification and tracking of individuals. DARPA has already funded its "Human ID at a Distance" program, which aims to positively identify people from a distance through technologies such as face recognition or gait recognition. A nationwide identification system would be of great assistance to such a project by providing an easy means to track individuals across multiple information sources.

DARPA's Broad Agency Announcement 02-08 soliciting proposals from industry states that the initial plan is for a five year research project into these various technologies. The interim goal is to build "leave-behind prototypes with a limited number of proof-of-concept demonstrations in extremely high risk, high payoff areas." The FBI and the Transportation Security Administration are also working on data-mining projects that will fuse commercial databases, public databases, and intelligence data and had meetings with TIA developers.

WILLIAM SAFIRE

You Are a Suspect

WASHINGTON

If the Homeland Security Act is not amended before passage, here is what will happen to you:

Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade your receive, every bank deposit you make, every trip you book and every event you attend — all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."

To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you — passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the latest hidden camera surveillance — and you have the supersnoop's dream: a "Total Information Awareness" about every U.S. citizen.

This is not some far-out Orwellian scenario. It is what will happen to your personal freedom in the next few weeks if John Poindexter gets the unprecedented power he seeks.

Remember Poindexter? Brilliant man, first in his class at the Naval Academy, later earned a doctorate in physics, rose to national security adviser under President Ronald Reagan. He had this brilliant idea of secretly selling missiles to Iran to pay ransom for hostages, and with the illicit proceeds to illegally support contras in Nicaragua.

A jury convicted Poindexter in 1990 on five felony counts of misleading Congress and making false statements, but an appeals court overturned the verdict because Congress had given him immunity for his testimony. He famously asserted, "The buck stops here," arguing that the White House staff, and not the president, was responsible for fateful decisions that might prove embarrassing.

This ring-knocking master of deceit is back again with a plan even more scandalous than Iran-contra. He heads the "Information Awareness Office" in the otherwise excellent De-

fense Advanced Research Projects Agency, which spawned the Internet and stealth aircraft technology. Poindexter is now realizing his 20-year dream: getting the "data-mining" power to snoop on every public and private act of every American.

Even the hastily passed U.S.A. Patriot Act, which widened the scope of the Foreign Intelligence Surveillance Act and weakened 15 privacy laws, raised requirements for the government to report secret eavesdropping to Congress and the courts. But Poindexter's assault on individual privacy rides roughshod over such oversight.

He is determined to break down the wall between commercial snooping and secret government intrusion. The disgraced admiral dismisses such necessary differentiation as bureaucratic "stovepiping." And he has been given a $200 million budget to create computer dossiers on 300 million Americans.

When George W. Bush was running for president, he stood foursquare in defense of each person's medical, financial and communications privacy. But Poindexter, whose contempt for the restraints of oversight drew the Reagan administration into its most serious blunder, is still operating on the presumption that on such a sweeping theft of privacy rights, the buck ends with him and not with the president.

This time, however, he has been seizing power in the open. In the past week John Markoff of The Times, followed by Robert O'Harrow of The Washington Post, have revealed the extent of Poindexter's operation, but editorialists have not grasped its undermining of the Freedom of Information Act.

Political awareness can overcome "Total Information Awareness," the combined force of commercial and government snooping. In a similar overreach, Attorney General Ashcroft tried his Terrorism Information and Prevention System (TIPS), but public outrage at the use of gossips and postal workers as snoops caused the House to shoot it down. The Senate should now do the same to this other exploitation of fear.

The Latin motto over Poindexter's new Pentagon office reads "Scientia Est Potentia" — "knowledge is power." Exactly: the government's infinite knowledge about you is its power over you. "We're just as concerned as the next person with protecting privacy," this brilliant mind blandly assured The Post. A jury found he spoke falsely before. □

E-mail: safire@nytimes.com

Individual Liberty,
Limited Government,
Free Markets and Peace

Search
GO
Advanced Search
Help

Terrorism
- Terrorism Home
- The Military Response
- The Diplomatic Response
- Civil Liberties
- Bioterror and Other Future Threats
- Economic Impact
- Political Impact
- America's Values under Attack
- Press Information

Contribute
- Make a Contribution
- About Sponsorship
- Alternative Giving Methods
- Levels and Benefits

Cato Offerings

The USA Patriot Act: We Deserve Better

by Robert A. Levy, Senior Fellow in Constitutional Studies, Cato Institute

A version of this article orginally appeared in *Liberty* magazine.

If you think the Bill of Rights is just so much scrap paper, and the separation of powers doctrine has outlived its usefulness, then the USA PATRIOT Act, passed overwhelmingly on Oct. 25, is the right recipe to deal with terrorists. On the other hand, if you are concerned about Fifth Amendment protection of due process, and Fourth Amendment safeguards against unreasonable searches and seizures, then you should be deeply troubled by the looming sacrifice of civil liberties at the altar of national security.

To be sure, the Constitution is not a suicide pact. Government is legitimately charged with defending life, liberty, and property against both domestic and foreign predators. First among those obligations is to protect life. With America under attack, and lives at risk, civil liberties cannot remain inviolable. But that's a far cry from asserting that they may be flouted to wage war against fanatics.

Proponents of the new bill surely understood that many of its provisions were incompatible with civil liberties. Yet rather than modify the offending provisions, the president and Congress decided to promote the bill as an expression of patriotism. Hence the acronym - USA PATRIOT - and its bloated title, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The sales pitch worked. Fearful of being labeled disloyal after the September atrocities, the House endorsed the bill 357-to-66, followed by a 98-to-1 rout in the Senate, with only Russ Feingold (D-Wis.) in opposition.

From its initial draft to its final adoption, USA PATRIOT zipped through in six weeks - gutting much of the Fourth Amendment in far less time than Congress typically expends on routine bills that raise no constitutional concerns. Congress' so-called deliberative process was reduced to this: Closed-door negotiations; no conference committee; no committee reports; no final hearing at which opponents could testify; not even an opportunity for most of the legislators to read the 131 single-spaced pages about to become law. Indeed, for part of the time, both the House

May 6, 2003

Daily Commentary
Homeland Security: Follow the Bouncing Ball
by Charles V. Peña

Minority Rules: Filibustering the Constitution
by James L. Swanson

[Archives]

Daily Dispatch
- Bush Trying to Stop North Korea from Exporting Nuclear Material
- New Legislation Would Protect Gun Industry From Lawsuits
- Pakistan Will Disarm Nukes if India Does

[Archives]

Live This Week
May 7, 2003
The Real Environmental Crisis: Why Poverty, Not Affluence, Is the Environment's Number One Enemy
11:00 a.m.
Cato Book Forum

Scholar Interviews

The USA Patriot Act: We Deserve Better

by Robert A. Levy, Senior Fellow in Constitutional Studies, Cato Institute

A version of this article orginally appeared in *Liberty* magazine.

If you think the Bill of Rights is just so much scrap paper, and the separation of powers doctrine has outlived its usefulness, then the USA PATRIOT Act, passed overwhelmingly on Oct. 25, is the right recipe to deal with terrorists. On the other hand, if you are concerned about Fifth Amendment protection of due process, and Fourth Amendment safeguards against unreasonable searches and seizures, then you should be deeply troubled by the looming sacrifice of civil liberties at the altar of national security.

To be sure, the Constitution is not a suicide pact. Government is legitimately charged with defending life, liberty, and property against both domestic and foreign predators. First among those obligations is to protect life. With America under attack, and lives at risk, civil liberties cannot remain inviolable. But that's a far cry from asserting that they may be flouted to wage war against fanatics.

Proponents of the new bill surely understood that many of its provisions were incompatible with civil liberties. Yet rather than modify the offending provisions, the president and Congress decided to promote the bill as an expression of patriotism. Hence the acronym - USA PATRIOT - and its bloated title, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The sales pitch worked. Fearful of being labeled disloyal after the September atrocities, the House endorsed the bill 357-to-66, followed by a 98-to-1 rout in the Senate, with only Russ Feingold (D-Wis.) in opposition.

From its initial draft to its final adoption, USA PATRIOT zipped through in six weeks - gutting much of the Fourth Amendment in far less time than Congress typically expends on routine bills that raise no constitutional concerns. Congress' so-called deliberative process was reduced to this: Closed-door negotiations; no conference committee; no committee reports; no final hearing at which opponents could testify; not even an opportunity for most of the legislators to read the 131 single-spaced pages about to become law. Indeed, for part of the time, both the House and Senate were closed because of the anthrax scare; congressional staffers weren't able to access their working papers.

The negligible legislative record will make it difficult for courts to determine the intent of Congress. And because legislative intent matters to some judges - for example, Supreme Court Justices Stephen Breyer and David Souter - the USA PATRIOT statute might ultimately be invalidated as unconstitutionally vague. Ironically, Congress' rush job, which facilitated passage of the bill, could be the cause of the bill's downfall. The same law that was promoted as an act of patriotism might even provide a rationale for releasing the madmen who committed the horrific terrorist acts against the United States.

Yet the more acute objections to the new statute are substantive, not procedural. They fall into three main categories. First, any law with the potential to dramatically alter conventional notions of individual freedom should fastidiously guard against abuse. The doctrine of separation of powers, a centerpiece of our Constitution, has been a traditional buffer against such abuse. By requiring advance judicial authorization of certain executive actions, followed by judicial review to assure that those actions have been properly performed, our liberties are shielded from excessive concentrations of power in a single branch of government. As we shall see, the USA PATRIOT Act does not pass muster.

Second, if the new rules are at all justifiable, they are defended as a necessary instrument of anti-terrorism. If so, why do many of the provisions apply not only to suspected terrorist acts but also to everyday national security investigations and even ordinary criminal matters? In effect, our government has exploited the events of Sept. 11 to impose national police powers that skirt time-honored constraints on the state. The executive branch will not always wield its new powers in the service of ends that Americans find congenial. Better that the government be shackled by the chains of the Constitution.

Third, laws that compromise civil liberties must be revisited periodically to assure that temporary measures, undertaken in response to a national security emergency, do not endure longer than necessary. Such laws must contain sunset clauses; that is, the law should expire automatically within a short time of enactment - thus imposing on government the continuing obligation to justify its intrusions. In this instance, the Bush Administration rejected any sunset provision whatsoever. Congress demurred, and insisted on including such a provision; but it applied only to new wiretap and surveillance powers, not to the whole bill. Moreover, the sunset date was fixed at Dec. 31, 2005 - more than four years after passage of the legislation. Plainly, a shorter time frame - one year, or two years at most - would have been appropriate. If the emergency persisted, Congress and the president could reenact the law.

Skeptics might dismiss those objections as mere abstractions - civil libertarianism run amok - unless they are illuminated by concrete examples from the statute. Here, then, are just a few of the more egregious threats to personal freedom.

During the Carter administration, Congress passed the Foreign Intelligence Surveillance Act, which created a new federal court to approve electronic surveillance of citizens and resident aliens alleged to be acting on behalf of a foreign power. Until now, the FISA court granted surveillance authority if foreign intelligence was the primary purpose of an investigation. No longer. Under Section 218 of the USA PATRIOT Act, foreign intelligence need only be "a significant purpose" of an investigation. That sounds like a trivial change, but it isn't. Because the standard for FISA approval is lower than "probable cause," and because FISA now applies to ordinary criminal matters if they are dressed up as national security inquiries, the new rules could open the door to circumvention of the Fourth Amendment's warrant requirements. The result: rubber-stamp judicial supervision of phone and Internet surveillance, even in regular criminal cases, and FBI access to medical, educational, and other business records that might conceivably relate to foreign intelligence probes.

The FISA revision is but one example of the government's expanded powers to conduct searches and surveillance. There are others. Government will have access to some financial records, without notice or judicial review. While judicial approval is necessary to retrieve voicemail messages, the requisite court order can now be obtained with a minimal showing of relevancy. That same low standard governs traces on Internet surfing and email. Perhaps worst of all, under Section 213 of the Act, secret "sneak and peek" searches of physical property will be condoned in routine criminal investigations. Those searches can be conducted without knowledge of the property owner until a "reasonable" time after the search has occurred. No knowledge means no opportunity to contest the validity of the search, including such obvious infractions as rummaging through office drawers when the warrant authorizes a garage search, or even searching the wrong address.

On the money laundering front (Sections 301 through 377), the secretary of the treasury is empowered to label any jurisdiction a "primary money laundering concern," in which case foreign banks will be required to disclose their customers and transactions. Predictably, the identified countries will be those with low tax structures and strict financial privacy laws. Yet there is little evidence that tax havens are

a magnet for dirty money. In fact, when money is transferred across borders and back again, the risk of detection is high. That serves as a deterrent to such transactions. To punish nations that harbor terrorists and their assets, we should shut off U.S. access to financial institutions that refuse to provide evidence associated with the September carnage. We should also invoke existing bilateral agreements, and negotiate new agreements, waiving bank secrecy and requiring mutual cooperation when prosecuting terrorist acts.

Finally, civil libertarians are rightly alarmed that the attorney general can detain, for seven days, non-citizens suspected of terrorism. After seven days, pursuant to Section 412 of the Act, deportation proceedings must commence or criminal charges must be filed. Originally, the Justice Department had asked for authority to detain suspects indefinitely without charge. Congress could not be persuaded to go along. But the final bill, for all practical purposes, allows expanded detention simply by charging the detainee with a technical immigration violation. And if a suspect cannot be deported, he can still be detained if the attorney general certifies every six months that national security is at stake.

To illustrate the magnitude and scope of that problem, the *Wall Street Journal* reported on Nov. 1 that seven Democrats had filed Freedom of Information Act requests for a detailed accounting from Attorney General John Ashcroft on the status of more than 1,000 detainees. The lawmakers cited reports that "some detainees have been denied access to their attorneys, proper food, or protection from ... physical assault." Some of them were allegedly being held in solitary confinement even though they hadn't been charged with any criminal offense. According to a representative of the New York Legal Aid Society, several Arab detainees had been limited to one phone call per week to a lawyer and, if the line was busy, they had to wait another week.

Maybe those reports will turn out to be groundless. But it's time for some answers. Here's what the *Washington Post* had to say in an Oct. 31 editorial: "The Department of Justice continues to resist legitimate requests for information regarding the 1,017 people it acknowledges having detained in its investigation of the September 11 attacks.... The questions are pretty basic. How many of the 1,000-plus are still in custody? Who are they? What are the charges against them? What is the status of their cases? Where and under what circumstances are they being held? The department refuses not only to provide the answers but also to give a serious explanation of why it won't provide them."

Ultimately, the Supreme Court may have to clarify how the civil liberties / national security tradeoff will unfold. This past term, in *Zadvydas v. Underdown*, the Court held that immigrants who have committed crimes cannot be detained indefinitely, but must be deported within a reasonable period or released. Moreover, said the Court, temporary and even illegal immigrants, not just U.S. citizens, are entitled to due process. Still, the Court noted that different rules may apply to immigrants who are denied entry, suspected of terrorism, or considered to be national security risks.

Thus, the law is murky; and the legislation passed in the aftermath of September's events adds new elements of uncertainty. Nonetheless, the controlling principle is unambiguous. Any attempt by government to chip away at constitutionally guaranteed rights must be subjected to the most painstaking scrutiny to determine whether less invasive means could accomplish the same ends. The USA-PATRIOT anti-terrorism bill does not survive that demanding test. In a free society, we deserve better.

USAPATRIOT

SEC. 802. DEFINITION OF DOMESTIC TERRORISM.

(a) DOMESTIC TERRORISM DEFINED- Section 2331 of title 18, United States Code, is amended--

(1) in paragraph (1)(B)(iii), by striking `by assassination or kidnapping' and inserting `by mass destruction, assassination, or kidnapping';

(2) in paragraph (3), by striking `and';

(3) in paragraph (4), by striking the period at the end and inserting `; and'; and

(4) by adding at the end the following:

`(5) the term `domestic terrorism' means activities that--

`(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

`(B) appear to be intended--

`(i) to intimidate or coerce a civilian population;

`(ii) to influence the policy of a government by intimidation or coercion; or

`(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

`(C) occur primarily within the territorial jurisdiction of the United States.'.

if you or your legal partner sends dues to an organization so defined, you are liable

organizations or acts that could qualify:

- PETA
- the tree-sitters in the North West
- Operation Rescue
- motorcycle groups
- militias
- any public demonstration during which a few trouble-makers set off a coercive police response
- strike actions, ditto

SEC. 507. DISCLOSURE OF EDUCATIONAL RECORDS.

Section 444 of the General Education Provisions Act (20 U.S.C. 1232g), is amended by adding after subsection (i) a new subsection (j) to read as follows:

`(j) INVESTIGATION AND PROSECUTION OF TERRORISM-

`(1) IN GENERAL- Notwithstanding subsections (a) through (i) or any provision of State law, the Attorney General (or any Federal officer or employee, in a position not lower than an Assistant Attorney General, designated by the Attorney General) may submit a written application to a court of competent jurisdiction for an ex parte order requiring an educational agency or institution to permit the Attorney General (or his designee) to--

`(A) collect education records in the possession of the educational agency or institution that are relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of title 18 United States Code, or an act of domestic or international terrorism as defined in section 2331 of that title; and

`(B) for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such records, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.

`(2) APPLICATION AND APPROVAL-

`(A) IN GENERAL- An application under paragraph (1) shall certify that there are specific and articulable facts giving reason to believe that the education records are likely to contain information described in paragraph (1)(A).

`(B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).

`(3) PROTECTION OF EDUCATIONAL AGENCY OR INSTITUTION- An educational agency or institution that, in good faith, produces education records in accordance with an order issued under this subsection shall not be liable to any person for that production.

`(4) RECORD-KEEPING- Subsection (b)(4) does not apply to education records subject to a court order under this subsection.'.

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';

(2) by inserting `, routing, addressing,' after `dialing'; and

(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

`(a) IN GENERAL-

`(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

`SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

`(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

`(2) An investigation conducted under this section shall--

`(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

`(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

`(b) Each application under this section--

`(1) shall be made to--

`(A) a judge of the court established by section 103(a); or

`(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

`(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

`(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

`(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

SEC. 508. DISCLOSURE OF INFORMATION FROM NCES SURVEYS.

Section 408 of the National Education Statistics Act of 1994 (20 U.S.C. 9007), is amended by adding after subsection (b) a new subsection (c) to read as follows:

'(c) INVESTIGATION AND PROSECUTION OF TERRORISM-

'(1) IN GENERAL- Notwithstanding subsections (a) and (b), the Attorney General (or any Federal officer or employee, in a position not lower than an Assistant Attorney General, designated by the Attorney General) may submit a written application to a court of competent jurisdiction for an ex parte order requiring the Secretary to permit the Attorney General (or his designee) to--

'(A) collect reports, records, and information (including individually identifiable information) in the possession of the center that are relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of title 18, United States Code, or an act of domestic or international terrorism as defined

'(B) for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such information, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.

'(2) APPLICATION AND APPROVAL-

'(A) IN GENERAL- An application under paragraph (1) shall certify that there are specific and articulable facts giving reason to believe that the information sought is described in paragraph (1)(A).

'(B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).

'(3) PROTECTION- An officer or employee of the Department who, in good faith, produces information in accordance with an order issued under this subsection does not violate subsection (b)(2) and shall not be liable to any person for that production.'.

'Sec. 626. Disclosures to governmental agencies for counterterrorism purposes

'(e) SAFE HARBOR- Notwithstanding any other provision of this title, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a governmental agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.'.

SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.

Section 3103a of title 18, United States Code, is amended--

(1) by inserting `(a) IN GENERAL- ' before `In addition'; and

(2) by adding at the end the following:

`(b) DELAY- With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if--

`(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);

`(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

`(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.'.

SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.

(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-

(1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:

'(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.'.

http//legis.state.nm.us/Sessions/03%20Regular/memorials/house/HJM040.html

46th legislature - STATE OF NEW MEXICO - first session, 2003 INTRODUCED BY Max Coll

A JOINT MEMORIAL

AFFIRMING CIVIL RIGHTS AND LIBERTIES; DECLARING OPPOSITION TO FEDERAL MEASURES THAT INFRINGE ON CIVIL LIBERTIES.

WHEREAS, the state of New Mexico is proud of its long and distinguished tradition of protecting the civil rights and liberties of its residents; and

WHEREAS, New Mexico has a diverse population, including immigrants and students, whose contributions to the community are vital to its economy,
culture and civic character; and

WHEREAS, the preservation of civil rights and liberties is essential to the well-being of a democratic society; and

WHEREAS, federal, state and local governments should protect the public from terrorist attacks such as those that occurred on September 11, 2001 and should do so in a rational and deliberative fashion to ensure that a new security measure will enhance public safety without impairing constitutional rights or infringing on civil liberties; and

WHEREAS, government security measures that undermine fundamental rights do damage to American institutions and values that the residents of New Mexico hold dear; and

WHEREAS, the house of representatives believes that there is no inherent conflict between national security and the preservation of liberty and that Americans can be both safe and free; and

WHEREAS, federal policies adopted since September 11, 2001, including provisions in Public Law 107-56, known as the USA Patriot Act, and related executive orders, regulations and actions threaten fundamental rights and liberties by

A. authorizing the indefinite incarceration of non-citizens based on mere suspicion and the indefinite incarceration of citizens designated by the president as "enemy combatants" without access to counsel or meaningful recourse to the federal courts;

B. limiting the authority of federal courts to curb law enforcement abuse of electronic surveillance in anti-terrorism and ordinary criminal investigations;

C. expanding the authority of federal agents to conduct so-called "sneak and peek" or "black bag" searches, in which the subject of the search warrant has not been notified that his or her property has been searched;

D. granting federal law enforcement and intelligence agencies broad access to personal, medical, financial, library and educational records with little, if any, judicial oversight;

E. chilling constitutionally protected speech through overly broad definitions of "terrorism";

F. driving a wedge between immigrant communities and the police that protect them by encouraging involvement of state and local police in the enforcement of federal immigration law; and

G. permitting the federal bureau of investigation to conduct surveillance of religious services, internet chat rooms, political demonstrations and public meetings of any kind without evidence that a crime has been or may be committed; and

WHEREAS, these new powers pose a particular threat to the civil rights and liberties of the residents of New Mexico state who are or who are assumed to be Arab, Muslim or of South Asian descent; and

WHEREAS, other communities throughout the country have enacted resolutions reaffirming support for civil rights and civil liberties in the face of government policies that threaten these values and have demanded accountability from law enforcement agencies regarding their use of these new powers;

NOW, THEREFORE, BE IT RESOLVED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO that it

A. affirm its strong support for fundamental constitutional rights and its opposition to federal measures that infringe on these rights and liberties;

B. affirm its strong support for the rights of immigrants and oppose measures that single out individuals for legal scrutiny or enforcement activity based on their country of origin;

C. direct the New Mexico state police to

(1) refrain from participating in the enforcement of federal immigration laws;

(2) seek adequate written assurances from federal authorities that residents of the state of New Mexico and individuals in the custody of the state who are placed in federal custody will not be subjected to military or secret detention or secret immigration proceedings without access to counsel and, absent such written assurances, refrain from assisting federal authorities to obtain custody of these individuals;

(3) refrain from engaging in the surveillance of individuals or groups of individuals based on their participation in activities protected by the First Amendment to the United States constitution, such as political advocacy or the practice of a religion, without reasonable and particularized suspicion of criminal conduct unrelated to the activity protected by the First Amendment to the United States constitution;

(4) refrain from using race, religion, ethnicity or national origin as a factor in selecting who is subject to investigatory activities unless race, religion, ethnicity or national origin is part of the description of a specific suspect to be apprehended;

(5) refrain, whether acting alone or with federal law enforcement officers, from collecting or maintaining information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activity and there are reasonable grounds to believe that the subject of the information is or may be involved in criminal conduct;

(6) provide advance or simultaneous notice of the execution of a search warrant to any resident of the state of New Mexico whose property is the subject of the search and refrain from participating in a joint search with any law enforcement agency absent assurances that such a notice will be provided;

(7) refrain from undertaking or participating in any initiative, such as the terrorist information and prevention system, also known as TIPS, that encourages members of the general public to spy on their neighbors, colleagues or customers;

(8) refrain from the practice of stopping drivers or pedestrians for the purpose of scrutinizing their identification documents without reasonable and particularized suspicion of criminal activity; and

(9) report to the legislature and the interim corrections oversight and justice committee, any request by federal authorities that, if granted, would cause agencies of the state to exercise powers or cooperate in the exercise of powers in apparent violation of a city ordinance or the laws or constitution of this state or of the United States;

D. direct public schools and institutions of higher education to provide notice to individuals whose education records have been obtained by law enforcement agents pursuant to Section 507 of the USA Patriot Act;

E. direct public libraries to post in a prominent place within the library a notice as follows "WARNING

Under Section 215 of the federal USA Patriot Act (Public Law 107-56), records of books and other materials you borrow from this library may be obtained by federal agents. This law also prohibits librarians from informing you if records about you have been obtained by federal agents. Questions about this policy should be directed to Attorney General John Ashcroft, Department of Justice, Washington, DC 20530."; and

F. direct the state official in charge of homeland security for New Mexico to seek periodically from federal authorities the following information in a form that facilitates an assessment of the effect of federal anti-terrorism efforts on the residents of the state of New Mexico and provide to the legislature and the interim corrections oversight and justice committee, no less than once every six months, a summary of the information obtained

(1) the names of all residents of New Mexico who have been arrested or otherwise detained by federal authorities as a result of terrorism investigations since September 11, 2001, and

(a) the location of each detainee;

(b) the circumstances that led to each detention;

(c) the charges, if any, lodged against each detainee; and

(d) the name of counsel, if any, representing each detainee;

(2) the number of search warrants that have been executed in New Mexico without notice to the subject of the warrant pursuant to Section 213 of the USA Patriot Act;

(3) the extent of electronic surveillance carried out in the state pursuant to powers granted in the USA Patriot Act;

(4) the extent to which federal authorities are monitoring political meetings, religious gatherings or other activities within New Mexico that are protected by the first Amendment of the United States constitution;

(5) the number of times education records have been obtained from public schools and institutions of higher learning in New Mexico pursuant to Section 507 of the USA Patriot Act;

(6) the number of times library records have been obtained from libraries in New Mexico pursuant to Section 215 of the USA Patriot Act; and

(7) the number of times records of books purchased by store patrons have been obtained from bookstores in New Mexico pursuant to Section 215 of the USA Patriot Act; and

BE IT FURTHER RESOLVED that copies of this memorial be transmitted to Senators Jeff Bingaman and Pete Domenici and Representatives Tom Udall, Heather Wilson and Steve Pearce, with a letter urging them to monitor federal anti-terrorism tactics and to work to repeal provisions of the USA Patriot Act and other laws and regulations that infringe on civil rights and liberties; and

BE IT FURTHER RESOLVED that copies of this memorial be transmitted to President George W. Bush and Attorney General John Ashcroft; and

BE IT FURTHER RESOLVED that a copy of this memorial be transmitted to the state official in charge of homeland security for New Mexico; and

BE IT FURTHER RESOLVED that copies of this memorial be transmitted to the New Mexico state police and to all public schools, institutions of higher education and public libraries within the state of New Mexico.

Search

Advanced Search
Help

Publications

- Books
- Policy Studies
- Cato Policy Report
- Cato Journal
- Regulation Magazine
- Cato Handbook for Congress
- Congressional Testimony
- Legal Briefs
- Cato Audio
- Cato's Letters
- To Be Governed...
- Events Archive

25th Anniversary

- 25th Home
- Friedman Prize
- Milton Friedman
- About Cato
- Cato Timeline

Contribute

- Make a Contribution
- About Sponsorship
- Alternative Giving Methods
- Levels and Benefits

Cato Daily

December 7, 2002

Total Information Awareness: Back to the Future

by Charles V. Peña

Charles V. Peña is senior defense policy analyst at the Cato Institute.

The idea of "total information awareness," or TIA, has come under fire lately. And for good reason. This new system for intelligence gathering could backfire and lead to a repetition of the intelligence failures America experienced prior to 9/11.

TIA is a Pentagon program designed to build a large-scale counter-terrorism database from myriad sources, including e-mail, electronic and credit card purchases, airline travel, rental cars, telephone calling cards, gun purchases, and medical records.

Supporters argue that it's an advanced computer tool intended to help catch would-be terrorists by looking for links and patterns indicative of terrorist activity. Critics are concerned that the TIA program would be the first step towards a surveillance state and allow the U.S. government to monitor and spy on its own citizens. For example, some critics have written the following:

- "[W]e do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?"

- "The administration's interest in e-mail is a wholly unhealthy precedent, especially given this administration's track record on FBI files and IRS snooping. Every medium by which people communicate can be subject to exploitation by those with illegal intentions. Nevertheless, this is no reason to hand Big Brother the keys to unlock our e-mail diaries, open our ATM records, read our medical records, or translate our international communications."

You would think such "alarmist" rhetoric is coming from groups such as the American Civil Liberties Union, the Electronic Privacy Information Center, or the Southeastern Legal Foundation -- all of whom have been critical of TIA.

You would be wrong.

January 2, 2003

Daily Commentary

Interventionism, Allegedly a Middle-of-the-Road Policy

by Ludwig von Mises

[Archives]

Daily Digest

- South Korea and China Act Diplomatically with North Korea
- D.C. Cuts Literacy Program
- New Study Says Global Warming is Forcing Many Species to Migrate

[Archives]

Pocket Constitution
Email Updates
Cato Audio
Cato Store
Cato on Your PDA
Cato University
El Cato

Those words were written in October 1997 by then-Senator John Ashcroft. He was taking issue with the Clinton administration's views on the Internet and proposed regulations and controls. Curiously, today, Attorney General Ashcroft has been deafeningly silent on the issue of TIA. Apparently, what's not good for the goose is okay for the gander.

But Ashcroft's concerns about the future of the Internet then are as valid when it comes to TIA now. Americans should not blindly give in to fear and a sense of vulnerability by giving the federal government (in particular, the executive branch) ever-expansive powers all in the name of homeland security and fighting the war on terrorism. The fundamental question is not whether TIA is a good idea right now because we must cope with a new terrorist threat. The question is whether TIA is a good idea, period -- whether in this, the previous, or successive administrations.

Concerns about TIA are threefold.

First and foremost is the issue of civil liberties. If government had a pristine record and this was the first and only proposal that potentially threatens civil liberties, perhaps the cause for concern might be less. But TIA is being proposed by an administration with a penchant for secrecy and a "trust us, we know what we're doing" attitude. This same administration also gave us the USA PATRIOT Act, which gives the executive branch extraordinary power absent judicial checks and balances. And even though it was explicitly prohibited in the Homeland Security Act, the administration had previously proposed the TIPS (Terrorist Information and Prevention System), which would have made us a nation of snitches.

Second, how might TIA affect the information economy and electronic commerce? TIA is built on the premise of having access to transactional and record-keeping data. But people need to know that private information handed over to Internet service providers, banks, airlines, hotels, and other businesses will not routinely be given to the government and stored in a centralized database that -- despite cybersecurity -- could be hacked.

Third, how effective would TIA be in identifying and catching terrorists? TIA assumes that terrorists act according to certain patterns. If terrorist activity is static and unchanging, then the past could be predictive of the future. But the nature of terrorists is that they morph and adapt -- so they will likely learn the cues and patterns TIA is looking for and then avoid them. And this would increase the likelihood that TIA will mistakenly identify ordinary people as terrorists.

One final caution about TIA: It's being touted as a solution

to "connecting the dots" of intelligence data that weren't connected prior to Sept. 11. But another major intelligence shortcoming was over-reliance on technology and not enough human intelligence. The U.S. government needs to be careful about going back to the future with TIA and falling into the same trap.

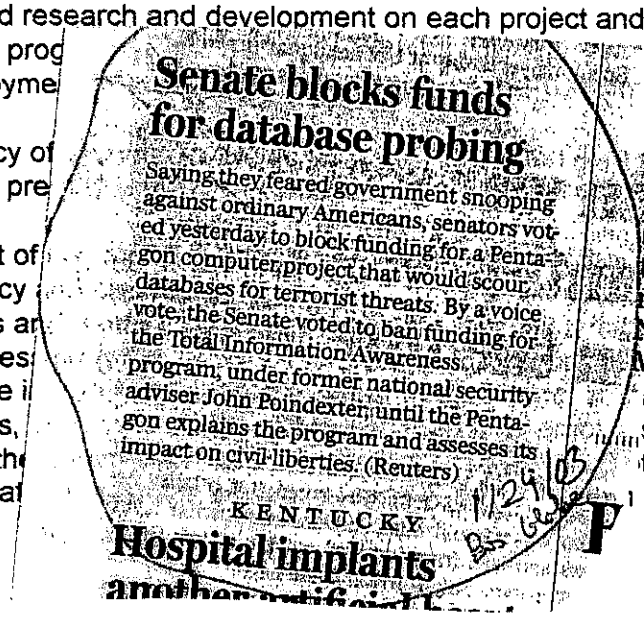
Send this page to a friend

Printer Friendly Version

1000 Massachusetts Avenue, N.W. Washington D.C. 20001-5403
Phone (202) 842-0200 Fax (202) 842-3490
All Rights Reserved © 2002 Cato Institute

From cdt.org:
Senate Votes to Block TIA Pending More Info - The US Senate approved on a voice vote an amendment blocking use of the Defense Department's Total Information Awareness program unless Congress specifically authorizes it after the Administration submits a report the amendment requires about the program and its effect on privacy. The amendment by Sen. Ron Wyden (D-OR) was added to the omnibus continuing appropriations act, the massive spending bill for fiscal 2003, now under consideration in the Senate. Jan. 23, 2003

Wyden Amendment
On 01/17/03, Sen. WYDEN (for himself, Mrs. FEINSTEIN, Mr. REID, Mrs. BOXER, Mr. CORZINE, and Mr. LEAHY) submitted Amendment 59 (SA 59) intended to be proposed by him to the joint resolution H.J. Res. 2, making further continuing appropriations for the fiscal year 2003, as follows:
At the end of title I of division M, add the following:
SEC. 111. (a) **LIMITATION ON USE OF FUNDS FOR RESEARCH AND DEVELOPMENT ON TOTAL INFORMATION AWARENESS PROGRAM.**--Notwithstanding any other provision of law, commencing 60 days after the date of the enactment of this Act, no funds appropriated or otherwise made available to the Department of Defense, whether to an element of the Defense Advanced Research Projects Agency or any other element, or to any other department, agency, or element of the Federal Government, may be obligated or expended on research and development on the Total Information Awareness program unless--
(1) the report described in subsection (b) is submitted to Congress not later than 60 days after the date of the enactment of this Act; or
(2) the President certifies to Congress in writing, that--
(A) the submittal of the report to Congress within 60 days after the date of the enactment of this Act is not practicable; and
(B) the cessation of research and development on the Total Information Awareness program would endanger the national security of the United States.
(b) **REPORT.**--The report described in this subsection is a report, in writing, of the Secretary of Defense, the Attorney General, and the Director of Central Intelligence, acting jointly, that–
(1) contains–
(A) a detailed explanation of the actual and intended use of funds for each project and activity of the Total Information Awareness program, including an expenditure plan for the use of such funds;
(B) the schedule for proposed research and development on each project and activity of the Total Information Awareness prog
(C) target dates for the deployme ormation Awareness program;
(2) assesses the likely efficacy of eness program in providing practically valuable pre r capabilities of terrorists or terrorist groups;
(3) assesses the likely impact of otal Information Awareness program on privacy
(4) sets forth a list of the laws ar e collected by the Total Information Awarenes ns of such laws that will be required to use the i program;
(5) includes recommendations, s, procedures, regulations, or legislation on th tal Information Awareness program to elimina on privacy and


Senate blocks funds for database probing

Saying they feared government snooping against ordinary Americans, senators voted yesterday to block funding for a Pentagon computer project that would scour databases for terrorist threats. By a voice vote, the Senate voted to ban funding for the Total Information Awareness program, under former national security adviser John Poindexter, until the Pentagon explains the program and assesses its impact on civil liberties. (Reuters)

1/24/03

KENTUCKY

Hospital implants

to "connecting the dots" of intelligence data that weren't connected prior to Sept. 11. But another major intelligence shortcoming was over-reliance on technology and not enough human intelligence. The U.S. government needs to be careful about going back to the future with TIA and falling into the same trap.

Send this page to a friend

Printer Friendly Version

1000 Massachusetts Avenue, N.W. Washington D.C. 20001-5403
Phone (202) 842-0200 Fax (202) 842-3490
All Rights Reserved © 2002 Cato Institute

Writ: Commentary

Front Page

Forums
Enron
Tribunals
Terrorism
2000 Elections

Archives
Columnists
Guest Columnists

Law Students

Book Reviews

Message Boards

Legal News
US Law
Supreme Court
Politics
Civil Rights
Crime
Tort
Business
Labor
Tech & IP
Environment

Investigations

International

Entertainment

Sports

News Wires

Legal Documents

FindLaw Features



Print This | Email This

Patriot II:

The Sequel Why It's Even Scarier than the First Patriot Act

By ANITA RAMASASTRY

Monday, Feb. 17, 2003

Soon after the terrorist acts of September 11, Congress passed the USA Patriot Act, which conferred broad new powers upon the federal government. Now John Ashcroft and his scribes at the Justice Department have been working secretly to create new, 120-page draft legislation that, if enacted, would expand greatly upon these already sweeping powers.

This daring sequel to the USA Patriot Act is known internally as the Domestic Security Enhancement Act. It is also nicknamed Patriot II (the name by which I'll refer to it here), or Son of Patriot. On February 7 of this year, a January 9 draft of Patriot II was revealed to the public - but not by the government. It was made public only through a leak.

Even Congress itself, strikingly, appears to have played little or no part in Patriot II's drafting (though it seems that Speaker of the House Hastert was, at least, given the opportunity to review the draft last month, as was Vice President Cheney.).

Perhaps the Bush Administration is looking to repeat its experience with the original USA Patriot Act. Amidst the emotional turmoil after September 11, the Administration introduced the Act and got it enacted in a matter of weeks. The Senate Judiciary Committee had only a brief, one-and-a-half-hour hearing on the Act, in which Attorney General Ashcroft testified but took no questions. In the House, meanwhile, there was no testimony from opponents of the bill.

After September 11, there was at least some rationale for this expedited consideration. Now, however, there is far less exigency. If the introduction of Patriot II in Congress coincides with the Iraq war, it may well be because the Administration has planned it that way, to take advantage of circumstances to ram the bill through both Houses quickly.

Even if Patriot II does end up being introduced in wartime, citizens and their representatives should fight this legislation tooth and nail, for it threatens to take even more of our liberties away. It is a wholesale assault on privacy, free speech, and freedom of

Coming W

Columnis
C. Dorf O
Supreme
Rejects
Racketee
Liability
Abortion

AND: Co
Anita Ra
On Chall
FBI's Spy

Book Revi

Michal B
The Vietn
Trial

- by Joan

Columnist

Akhil Am

Vikram A

Bart Aro

Sherry C

John Dea

Michael

Joanna G

Marci Ha

Julie Hild

Edward

Joanne M

Anita Ra

Supreme Court Center
Election 2000 Center
Recent Case Law
Cases & Codes
FindLaw Library
Legal Dictionary
MY FindLaw

information.

Making Total Information Awareness the Law

Admiral Poindexter's proposed Total Information Awareness (TIA) program, which sought to build data profiles of all Americans, sparked a wide public outcry. Congress recently warned against using TIA as a tool against US citizens. Nevertheless, Patriot II, as draft by the Attorney General and his staff, would begin to make TIA the law.

For instance, under Patriot II, federal agents would not need a subpoena or obtain a court order to access our consumer credit reports. This provision would open the wedge for TIA to be implemented through a huge database. Our credit reports are repositories of a great deal of sensitive information - from our employment history to where we shop, borrow and transact.

To see the information, the feds would only have to certify that they will use the information "in connection with their duties to enforce federal law." Note that they would not have to certify that the person whose information was accessed was suspected of terrorism, or indeed, any other crime. And no one would be notified that their records had been accessed. When a commercial entity requests a consumer's credit report, a note is made in the consumer's file alerting him to this fact.

A Mandate to Collect Genetic Information

Meanwhile, not only data, but genetic information would also be collected by the government if Patriot II were passed.

DNA would be put into a "Terrorist Identification Database." It would contain information not only for proven terrorists, but also "suspected terrorists." And that term would include anyone who was associated with, or had provided money or other support for, groups designated "terrorist."

It might also include protesters, or anyone else the government dislikes. Remember, the original USA Patriot Act defined the new crime of "domestic terrorism" broadly, to encompass "any action that endangers human life that is a violation of any Federal or State law."

Certainly one could envision a disruptive war protester who resisted arrest being tagged as a "suspected domestic terrorist," and forced to provide DNA. Would the government need to get a court order to procure the DNA? Not under Patriot II.

And what if the protester wouldn't comply? That would be a Class A misdemeanor, punishable by up to one year in prison and a $100,000 fine. Anyway, the protester's refusing to give up DNA might be futile - if any other government agency happens to have a blood sample, Patriot II gives the government the right to put it in the new database.

Incredibly, DNA would also be collected from anyone who is, or has been, on probation for any crime, no matter how minor. State governments would be required to collect DNA samples from state probationers and provide them to the federal government.

Anthony
Guest Co
Featured
Unmaskin
Throat

A W de w ev
identity of h
elusive new
by John D
Writ Forum
Message

Increasing Surveillance Powers

Database surveillance, under Patriot II, would also be combined with increased active surveillance of citizens.

To assess the change, it's important to remember that the Patriot Act itself already greatly expanded surveillance powers. Now Patriot II would, if enacted, makes it even easier for the government to engage in surveillance of U.S. citizens, without having to establish traditional probable cause under the Fourth Amendment. It would do so by making it easier for law enforcement to avail itself of the Foreign Intelligence Surveillance Court, which issues warrants more easily than federal district courts will.

The FISA Court is meant to address international terrorism, involving mostly noncitizens. Patriot II, however collapses the distinction between domestic and international terrorism, treating wholly domestic criminal acts as subject to the same, looser legal rules that apply to foreign intelligence gathering.

Remember, domestic terrorism is defined very broadly as "any action that endangers human life that is a violation of any Federal or State law." That means anything from getting into a raucous bar fight, to driving recklessly over the state speed limit, could theoretically count. And if the government finds a particular person suspicious, they could cite law violations as far from terrorism as these as a valid excuse for surveillance.

Worse, even those persons who cannot be deemed "domestic terrorists" because they have not broken any law, can alternatively be deemed "foreign powers" under Patriot II - even if they are American citizens or permanent residents. This allows the FBI to get pen registers on American citizens for a foreign intelligence investigation - without having to show any criminal or terrorist connection.

Gagging American Citizens and Cutting Off Their Rights to Sue

If you don't like the government's policies, including these, Patriot II says: Too bad. Don't try to make a federal case out of it - we'll bar you at the courthouse door.

What if you're lucky enough discover that you've been illegally spied on, in violation of your Fourth Amendment rights? Too bad. Patriot II would provide immunity from liability to law enforcement engaging in spying operations against the American people. The proposed act provides a defense for federal agents who engage unauthorized searches and surveillances relating to foreign intelligence when they are acting "pursuant to a lawful authorization from the President or the Attorney General."

What if a disgruntled business competitor chooses to falsely claim to the government that you're a "suspected terrorist"? Again, too bad. Don't consider suing the competitor, no matter what consequences ensure Patriot II eliminates civil liability for businesses and employees that report "suspected terrorists" to the federal government, no matter how malicious or unfounded the tip may be.

Like TIA, Operation TIPS - which would have enlisted government employees to spy on citizens - elicited public outcry. But this is TIPS

all over again. If they like, your package courier or cable guy can report you to the feds with impunity.

Broadly Criminalizing Encryption of Evidence

Meanwhile, in your search for a shred of privacy that might remain to you, don't even think about trying to protect your email. Under Patriot II, the government may go after you for that, too.

Specifically, Patriot II, as currently drafted, would makes it a new, separate crime to use encryption in the commission of another crime. To be convicted, the defendant must be shown to have "knowingly and willfully use[d] encryption technology to conceal any incriminating communication" relating to a federal felony he is committing, or attempting to commit.

The "federal crime" limitation may seem significant, until you realize that "domestic terrorism" - which can be based on a state law violation - is a federal crime. Remember, too, how loosely "domestic terrorism" is defined, in a way that could encompass a protester's resisting arrest, and if you do, you may reasonably fear using encryption even if you are not engaged in any criminal activity at all.

What if your encrypted email about protest planning is deemed "incriminating evidence" of your plan to resist arrest at the protest? You could be looking at five to ten.

The penalty for this offense alone would be up to ten years in prison. In addition, a Justice Department analysis included with the proposal suggests that the illegal encrypting ought to carry a mandatory minimum term of five years in prison.

Notably, the federal felony relating to the "incriminating communication" need not be an act of terrorism. It could be any federal crime, from the most major to the most minor, the most violent to the most excruciatingly technical. And that's frightening.

For instance, if a peer-to-peer website's users swap files, thus violating the Digital Millenium Copyright Act, and encrypt the files they are swapping, they may automatically face five years in prison, and could serve ten, for the encryption alone.

What is most shocking about the new encryption crime is that it is not limited to terrorism. This is the first attempt to regulate encryption domestically at all.

Shrouding Government Actions in Secrecy

While the government, according to Patriot II, has the right to know virtually everything about you, you have little right to know anything about the government.

Current grand jury secrecy rules apply only to jurors, prosecutors and courtroom staff. Patriot II would expand them to apply to witnesses too - meaning that ordinary citizens could not discuss their testimony with anyone but their attorney. In theory, they'd have to keep mum even with spouses or children, or face serious consequences.

What if they've been improperly subpoenaed in the first place? Under

Patriot II, too bad: Neither individuals nor organizations may move to try to quash a federal grand jury subpoena.

Will the grand jury itself at least remain independent? Nope. Patriot II allows the federal government to place gag orders on both federal and state grand juries, and to take over the proceedings.

Detentions will be similarly shrouded in an atmosphere of dead secrecy. The Justice Department's position on detainees is that if they are held incommunicado indefinitely without being charged with a crime, they need not be publicly identified. Patriot II would make that dubious position the law.

Meanwhile, if you do happen to somehow find out the identity or whereabouts of - or anything else about - a detainee, it would be criminal under Patriot II to reveal it. And that's the case even if you are the detainee's parent, spouse, or child.

Okay, you might ask, this is a lot of secrecy, but isn't it at least somewhat limited? Can't I at least use the Freedom of Information Act (FOIA) to figure out what the government is doing when it's not secretly detaining people, or secretly conducting grand jury proceedings?

No. Under Patriot II, FOIA would not extend to information "specifically exempted from disclosure by statute." What kind of statutes? Well, the USA Patriot Act might be one. Patriot II might be another.

It's a clever strategy: Collect private information. And then when citizens try to find out what you've collected, cite their own privacy right back at them as a reason not to divulge it.

If it seems farfetched to think the government could invoke privacy in this instance, consider that Ashcroft actually cited detainees' privacy as a reason not to release their names to the press, the public, or even their families.

Denaturalization: The Citizenship Death Penalty

In sum, Patriot II puts in jeopardy the First Amendment right to speak freely, statutory and common law rights to privacy, the right to go to court to challenge government illegality, and the Fourth Amendment right against unreasonable searches and seizures. But that's not all.

It also puts in jeopardy perhaps the most basic right of all: The right to walk the streets in safety without being "disappeared" by the government. Chileans have not always enjoyed this right. Americans, until now, always have.

Suppose you, as a citizen, attended a legal protest for which one of the hosts, unbeknownst to you, is an organization the government has listed as terrorist. Under Patriot II, you may be deported and deemed no longer an American citizen.

Under Patriot II, if you are simply suspected of terrorist activity, this can occur. More specifically, a U.S. citizen may be expatriated "if, with the intent to relinquish his nationality, he becomes a member of, or provides material support to, a group that the United Stated has

designated as a 'terrorist organization'."

How can you tell if the citizen wanted to relinquish citizenship? Under Patriot II, the intent can be inferred from conduct. So any association with even the legal activities of a designated group, plus any act that can be interpreted as disloyal to the United States, can mean you are deported, and no longer considered a citizen.

No Sunset Provisions for Patriot II Mean We Are Stuck with It If It Passes

The original USA Patriot Act has sunset provisions, under which the Act will expire if not renewed in five years. Patriot II, however, does not have such provisions. Indeed, it would go so far as to remove this important check from the original Patriot Act. So if Congress, and the American people don't focus carefully on Patriot II, even in the midst of impending war, we may be stuck with both Patriot Acts indefinitely.

Especially for that reason, Congress and the public need to learn more. Senator Patrick Leahy has argued, for instance, that before the Department of Justice asks Congress for more powers, it needs to disclose how it is using the ones it already has. Instead, the Department has so far repeatedly balked at both FOIA requests from the press and the public and requests from Congress for more detailed reporting pursuant to USA Patriot Act.

At the very least, Congress and the public should insist on a full understanding of what the Justice Department is doing before granting the executive branch still more authority via Patriot II .

What Do You Think? Message Boards

Anita Ramasastry is an Assistant Professor of Law at the University of Washington School of Law in Seattle and the Associate Director of the Shidler Center for Law, Commerce & Technology. Her prior columns on post-September 11 terrorism-related legislation can be found in the archive of her columns on this site.

FindLaw RESOURCES

LEGAL NEWS: Top Headlines · Supreme Court · Commentary · Crime · Cyberspace · International
US FEDERAL LAW: Constitution · Codes · Supreme Court Opinions · Circuit Opinions
US STATE LAW: State Constitutions · State Codes · Case Law
RESEARCH: Dictionary · Forms · LawCrawler · Library · Summaries of Law
LEGAL SUBJECTS: Constitutional · Intellectual Property · Criminal · Labor · more...
GOVERNMENT RESOURCES: US Federal · US State · Directories · more...
INTERNATIONAL RESOURCES: Country Guides · Trade · World Constitutions · more...
COMMUNITY: Message Boards · Newsletters · Greedy Associates Boards
TOOLS: Office · Calendar · Email · FAX · West WorkSpace · FirmSites

Advertising Info · Add URL · Help · Comments Jobs@FindLaw · Site Map

Company | Privacy Policy Disclaimer Copyright © 1994-2003 FindLaw

The Usa Patriot Act: One Year Later
Part II
by C. William Michaels*
t r u t h o u t | Report

Thursday, 14 November, 2002

The first part of this two-part article on the occasion of the first anniversary of the USA PATRIOT Act, looked at the background of the statute and reviewed some of its more significant sections among its very extensive ten Titles. This second part will review some of the trends occurring as a result of the USA PATRIOT Act and also identify some developments which will require attention in the foreseeable future.

Some Resulting Trends

There are any number of new trends and developments to be identified as coming directly from the PATRIOT Act itself. Of course, we cannot ignore numerous other developments, such as the Office of Homeland Security, dramatic new aviation security measures, several ominous national trends, and the impending war with Iraq, but unfortunately they are outside the present discussion as not being directly related to the PATRIOT Act. As to the Act, least 10 such trends could be noted, and they all deserve increased attention.

1. Reduced judicial review. The entire PATRIOT Act is designed for increased surveillance, information gathering, and investigation, of terrorism with a minimum of judicial review. Investigations under the Foreign Intelligence Surveillance Act (FISA) can be expanded and notification of sneak and peek warrants can be delayed. The FISA court which reviews and grants these warrant requests has refused perhaps 1 in its entire history, granting 12,178 warrants of 12,179 requests.

Under the PATRIOT Act, mostly under Title II, investigators can obtain information ranging from consumer reports, certain phone data, certain details from Internet service providers, educational records, and banking transactions, all without a court order. All that is required is a certification by a federal investigator that the information is necessary or required for a particular investigation, which does not even reach the standard of probable cause that is required with ordinary search and seizure warrants. There is no opportunity for judicial review of these information gathering activities since in general the information obtained is obtained in secret and the Act provides that the person or entity providing the information is immune from civil liability.

The Act's establishment of single jurisdiction search warrants and national service of search warrants effectively means that federal investigators only have to stop by to one federal district court to obtain a search warrant for a particular investigation. Investigators will not be required to further justify their information request and continue to meet search warrant standards in any other federal court even if the investigation goes into other jurisdictions. This is "one stop shopping" for federal search warrants and essentially takes the federal courts out of the loop.

The information sharing which will go on--and in fact is mandated--chiefly by Titles II and IX are conducted by and large without any judicial review. In those limited instances where judicial review might be involved, such review is limited to specific challenges and those challenges can be delayed at the request of the government.

The very extreme and detailed "special measures" which under Title III can be imposed by federal investigators upon domestic banks and other financial institutions are completely unprecedented in the history of federal banking regulation and represent a total rewrite of banking law. Yet these "special measures" can be submitted to banks by investigators once various required "certifications" are made by the Treasury Department, without any condition for a court order or court review. In fact, the Act does not even provide for a court review or challenge to a "special measures" order once imposed--and any given

"special measures" order can last for 120 days.

There is no provision in the Act for court review of the information which federal agencies can require from banks or financial institutions under the 120-hour rule established by the Act. In fact, no court would be able to review and properly pass upon the propriety of the information required, in that span of time.

Title IV of the Act identifies three types of terrorist organizations: "Section 219" designations of terrorist groups borrowed from existing immigration law, terrorist groups identified by the government under a similar procedure but with fewer requirements and no express judicial review, and a wide-ranging category of any group of two persons or more "whether organized or not" which engages in any of the broadly-defined list of "terrorist activities." Yet only one of them (adopting the "Section 219" designations from previous immigration law) allows for judicial review of a terrorist group designation. The second type of terrorist group, the PATRIOT Act describes a procedure similar to a "Section 219" terrorist group identification procedure, but any express reference to the same type of judicial review is curiously omitted in the statute's description. The third type of terrorist organization, any group organized or not which engages in terrorist activity, again contains no provision is for judicial review of that designation.

The Act therefore gives federal investigators or agencies tremendously wide latitude in designating terrorist groups--with all that would follow, once the entire range of the investigative and surveillance authorities also granted by the PATRIOT Act are brought into play against any group so identified. It must be noted that the definitions of "terrorism" and "domestic terrorism" and "foreign intelligence" do not exclude the potential involvement of American citizens, so PATRIOT Act investigation, surveillance, and prosecution, authorities are not restricted to aliens.

The mandatory detention of aliens under Title IV allows for habeas corpus review (similar, in fact, to other parallel provisions in existing immigration law although they were not as extreme). Yet habeas corpus review has not been utilized with great vigor by federal courts. An appeal of denial of habeas corpus is also provided, but such an appeal is extremely unlikely to succeed. Aside from habeas corpus, the only review allowed by an alien in indefinite detention is a request for administrative review of the detention, every six months. These provisions make a mockery of our system of judicial oversight of executive activity.

There is limited judicial oversight of many other Act provisions such as forfeiture provisions, long arm jurisdiction, and reduced or eliminated statutes of limitations. While these provisions may be seen as giving federal courts more power, in actuality the power is being given to federal prosecutors and investigators, who continue to drive federal criminal investigations and prosecutions.

2. Limited Congressional review or oversight. There are provisions scattered throughout the PATRIOT Act requiring various federal agencies or departments (chiefly State, Treasury, and Justice) to report to Congress on their activities or on the results of particular studies. Among them are reports to be made to Congress by the Treasury Department about "special measures" imposed on banks under Title III and by the Justice Department on the detention of aliens under Title IV.

Yet, little is said in the Act about Congressional power to take any action as a result of the reports. Also, little is said about the status of these various reports themselves, whether they are secret, how they can be distributed, if Congress has the power to restrict agency activity if Congress becomes concerned about information in them,, and so on. Congress itself, by enacting the PATRIOT Act, has withdrawn any authority it might have to oversee the results of the agency activity put into motion by its extreme provisions.

A prime example is the report to Congress on detention of aliens. The report only needs to include how many were detained at the start of the time period covered by the report, how many have been released, how many have sought judicial review of their detention, and how many are still detained. Notably absent from the requirements of this report are the names of the detainees, what each detainee may be charged

with, the circumstances of the detention, the locality of the detention, and whether criminal prosecution is underway. Again, Congress has abdicated its opportunity to exercise detailed oversight of such extreme provisions.

There has been some movement in the direction of Congressional oversight. For example, in June of 2002, Rep. F. James Sessenbrenner, Jr. and Rep. John Conyers, Jr. of the House Judiciary Committee sent an extensive letter to Attorney General John Ashcroft raising 50 rather pointed questions (many of those questions in several parts) about Justice Department activity related to the PATRIOT Act, especially Titles II and IV. The tone of this letter and its criticism of potential overbroad Executive Department conduct was commendable. But on the whole, Congressional action of this kind has been lackting. Much more is needed if Congress intends to exercise some control and oversight of the forces it set in motion with this Act.

3. "Fellow PATRIOT Acts." Congress surely is well aware that legislatures in the 50 States follow Congressional lead in identifying and acting on legislative priorities, from handguns to drunk driving. It has been no different in anti terrorism legislation. Within months after the PATRIOT Act was enacted by Congress and signed into law, other State legislatures acted on the mood of the country and the concern about terrorism investigation and considered if not passed similar State level legislation.

There are examples ranging from Maryland to California. In Maryland, new legislation rewrote State search and seizure guidelines, imposed new requirements on security for chemical plants and facilities, enacted new security measures for State office buildings (either by legislative act or Governor's order), and gave sweeping new powers to the Governor to declare special emergencies with subsequent powers for agencies dealing with health, transportation, policing, and security.

These "fellow PATRIOT Acts" pose problems no less severe than the Federal version. While perhaps not as extensive as the original, these other statutes are likely not to be interpreted with the same precision as might be imposed by federal courts, give new powers to certain State agencies ordinarily not accustomed to wielding them, and may not contain sunset provisions. Unfortunately, these State statutes and their effects will be with us for some time.

4. The "enemy combatant". A disturbing development among federal investigators is the announcement that a particular person seized and detained for suspected terrorist involvement or charged with a terrorism offense is a "enemy combatant." Even more alarming is the fact that this label has been used against a United States citizen. Investigators have made this announcement with arrests like Jose Padilla the so-called "dirty bomber" and his supposed accomplice, Adham Hassoun. Both were arrested in May and June, 2002 in Florida, and have been held in a Navy brig in North Carolina. Their eventual fate is still unknown. The government also has argued this theory in a brief filed in the United States Court of Appeals for the Fourth Circuit.

According to this approach, which has followed the wide investigative and detention authorities either established or expanded by the PATRIOT Act, an "enemy combatant" is not entitled to the same due process protections as any other detainee or arrestee. Such a person does not have the same rights to challenge their detention or to seek court review. Such a person can be held until the "conflict" is "concluded." If this is to mean the end of the "war on terrorism," then the time frame could be years. Yet this "enemy combatant" designation appears nowhere in the PATRIOT Act or in general federal criminal law. How this very alarming approach will be met by the courts is one of the major unfolding issues in the post-PATRIOT Act world.

5. Detention of aliens and detention conditions/the new American Gulag. The detention of aliens, now tremendously expanded by PATRIOT Act Title IV, and the conditions of their

detention, is one trend that fortunately continues to receive media and activist group attention. Many of the aliens seized and detained in roundups occurring immediately after September 11 and especially after the PATRIOT Act was signed, and which continue to occur, have been marked by serious deprivations of basic constitutional rights under the Fifth and Sixth Amendments, as well as rights and practices traditionally available to anyone in pretrial detention. Those include the rights to see family, to communicate with others, to meet with counsel, and to know of the charges being brought.

Stories coming from places like the Metropolitan Detention Center outside New York, federal detention facilities in Illinois near Chicago, and detention facilities in North Carolina (some of them military facilities) include other deprivations such as extreme conditions, solitary confinement, restrictions on food, beatings, and other brutalities. Many of the individuals seized and detained have little by way of family in this country, little or no financial resources, and only minimal knowledge of their own rights. The government is seizing the opportunity to exercise its considerable investigative, surveillance, and detention powers granted by the PATRIOT Act against a population that is least able effectively to respond.

The result, besides wholesale violations of the Constitution, protocols of detention, and human decency, is the potential development of a new American "gulag"--facilities where aliens or others seized under these expanded authorities will be placed and which can be relied upon by investigators to provide the proper conditions designed to elicit appropriate information by the arrestee useful in the investigation, not to mention confessions. Such a development if it occurs will be another black page on an already too-long history of extreme governmental treatment of suspect groups.

6. New "terrorist" group identifications globally/"their" terrorists become "our" terrorists. Part of the new globalization of the war on terrorism is activity by the United States seeking assistance or cooperation by other countries in investigating and tracking terrorist groups of immediate interest to the United States and who are suspected of involvement in the September 11 attacks, chiefly Al Queda. Of course, this interest also includes other terrorist groups so "designated" by United States authorities, which is already a tremendously long list.

In a show of further United States cooperation with these other nations, American authorities are also designating other groups in other countries which are deemed by these countries to be "terrorist" groups. In December, 2001 and on later dates, federal agencies announced that groups such as the Basque separatist movement in Spain (the ETA) and the Sendero Luminiso in Peru had been officially designated as "terrorist" groups for purposes of United States policy, notably invoking the considerable powers of surveillance, investigation, and prosecution granted by the PATRIOT Act.

Such groups clearly had nothing to do with September 11 although they have resorted to violence in their particular campaigns, but their official designation as a "terrorist" group has more to do with the United States recognizing another nation's "terrorists" in order to obtain that nation's assistance in acting against "terrorists" of interest to this country. That will soon develop into another disturbing trend of rebel groups of one sort or another in various countries being designated by the United States as "terrorists"--again, with all that entails in terms of surveillance and investigation. It is one way in which nations interested in preserving the status quo against the challenge of a dissident group can obtain the involvement and support of the United States and eliminating that group. How this plays out remains to be seen.

7. Using FISA material for criminal prosecution. The main reason why surveillance warrants under the Foreign Intelligence Surveillance Act are not subject to quite the same restrictions and requirements as search and seizure orders in other investigations is that FISA-type investigations are not designed to lead to direct criminal prosecution, but are expected to produce information to allow investigators to track the activities of certain suspect foreign

nationals under some sort of structure and guidelines. Yet after the PATRIOT Act, federal authorities are becoming more interested in using FISA investigations as the basis of a criminal investigation.

A recently-announced decision by the FISA court that was issued in May, 2002 (and was made public by the Senate Judiciary Committee–the first instance of a public FISA court opinion), criticized this approach. The FISA court in that opinion made it plain that it would be the arbiter of the FISA statute and how information obtained through FISA may be used. But the Justice Department has taken issue with that opinion. It has already taken the opinion up on appeal.

Using FISA information as the basis for standard criminal prosecution would go against the intent of FISA and would be, in effect, an end-run around the Fourth Amendment. This will be another trend to watch.

8. New information and surveillance technologies. As PATRIOT Act emphasis on surveillance and intelligence continues, so also will arise a whole new or expanded corporate subculture in surveillance technologies and methods. One example of this was quite evident in September 18 and 19, 2002, when a Homeland Security Technology Expo and Conference was held in Washington, D.C.

Hosted in part by the Department of Commerce in association with the Office of Homeland Security, this Tech Expo featured presentations, workshops, and displays by scores of technology-related firms involved in investigation, security, and surveillance. A sampling of these firms, whose particular expertise is indicated by the name alone, were: Ideal Shield, Language Analysis Systems, Biometric Key Systems, Dialogic Communication Corporation, Davidson Optronics, GM Defense/Patriot 3, Identicard Systems, QuickHire, Mindbank, WeGuardYou.com, and Vigilant Warning Systems.

This is only the beginning. A new generation of security and special electronic and surveillance methodology is about to unfold, some of which may have already been on the drawing board, but now given a serious boost by the studies, mandates, reports, grants, new offices, and special funding under the PATRIOT Act.

9. New corporate attitude as to employee surveillance. Congress may be well aware that the private sector/corporate world takes its lead from Congressional and White House interest and action on particular issues. The PATRIOT Act and the new emphasis on security is surely no exception.

Corporations, businesses, and merchants are now doing more than ever to track the movements of employees and customers, conduct background checks for new hires, review resumes, refuse hire to almost anyone with a criminal background even if it has nothing to do with the job involved, and track daily employee activities. Some computer surveillance programs in use in the corporate world allow a system administrator of a LAN to track keyboard keystrokes or even screen activity on any given computer in the system, down to whether the employee is conducting unauthorized shopping on the Internet (and this can even include credit card numbers entered) to slacking off by playing solitaire.

Some of these surveillance programs were already in use well before the PATRIOT Act. But the Act and the new atmosphere of security have given them a new legitimacy and have encouraged corporations either to expand or to institute similar surveillance systems. Keep in mind that if anything of any real import were discovered through these surveillance processes, its use in a criminal investigation is not restricted by the Fourth Amendment.

10. Reach of State and local authorities. The new PATRIOT Act provisions for information sharing, grants and funding, and cross agency training and cooperation, as well as the "fellow PATRIOT Acts" passed by State legislatures has given State and local governmental law enforcement units a new emphasis and a new influence.

Now, the county Sheriff or local municipal law enforcement unit may be involved in a terrorism investigation, can search for "foreign intelligence" and can watch out for "domestic terrorism." The professionalism of these organizations can sometimes be called into question, not to mention their lack of experience in these types of investigations. While that does not at all mean that it was a good thing for federal agencies to be given all of the new authorities provided by the PATRIOT Act, the expansion of these authorities to the State and local law enforcement levels is a disturbing "vertical expansion" of already disturbing police power.

Increased funding for everything. Not so much a trend as an observation, is the fact that the PATRIOT Act is part of an entire new federal and security apparatus due to receive, since September 11, an entire new wave of federal funding. It used to be that if a corporation was involved in drug enforcement, treatment, or surveillance, it was a prime recipient for federal contracts. Now the operative word is "terrorism" and corporations learn quickly. All sorts of new systems and mandates, contracts and grants, training and procedures, will be the subject for contracts at the federal, State and local levels. There already is enough funding in the PATRIOT Act to amount to $2.6 billion, not including "authorizations" without a specific sum. And that does not include funding for bioterrorism, which was the subject of a recently-enacted separate statute by Congress also recently signed by President Bush, aviation security (through the Aviation and Transportation Security Act which among many other things established the enormously large Transportation Security Administration), or increased military spending. The funding process is taking a new direction. It will be years before its effect is fully felt.

Watching for the Future

These 10 trends are enough for anyone interested in keeping abreast of immediate PATRIOT Act developments. But there are still four particular long-term matters to watch for in the foreseeable future.

1. "Domestic terrorism". The PATRIOT Act in Title VIII creates a new crime of "domestic terrorism." This is an act which is 1) a federal or State crime, 2) is dangerous or harmful to human life, 3) is designed to effect policy by coercion or intimidation, and 4) occurs within the United States. The intent of this new crime obviously is to "federalize" certain criminal acts and call them "terrorism" to bring them under federal surveillance, prosecution, and enhanced sentencing under the PATRIOT Act.

Civil liberties groups have raised concerns that "domestic terrorism" could include legitimate political protest, although the requirement that the action be dangerous or harmful to human life would place most political protest such as marches, demonstrations, and other activity, even if illegal, outside the definition. Also, to date, even a year since the PATRIOT Act no one has been prosecuted under the crime of "domestic terrorism."

Still, this is a development worth watching. How and in what way a prosecution for "domestic terrorism" would proceed clearly would show how the federal government will utilize that statute. Also, in a parallel way, the PATRIOT Act makes it clear that providing material support for, being in a conspiracy with, and attempting to commit, a terrorist act is also "terrorism." Prosecution of legitimate action such as political protest in support of a particular group or action, could be seen as terrorism under those definitions even if it is not prosecuted under the "domestic terrorism" crime. Both developments need to be watched.

2. Judicial review and oversight. Much has been made, even in this two-part series, of the lack of judicial oversight of government action in the PATRIOT Act. But it is a double-edged sword, for oversight and review of government action by the courts has not universally meant judicial restriction of that action. For example, the Alien and Sedition Acts enacted during World War I, the Espionage Act enacted subsequently, the detention of Japanese Americans during World War II, the actions of the House UnAmerican Activities Committee, and the Foreign Intelligence Surveillance Act, all were upheld by federal courts including the

> Supreme Court. So, if there is going to be judicial review and oversight, it needs to be materially different than historic judicial deference to Congressional conduct. It needs to be much more concerned with the Constitution than with Congress, with destruction of civil liberties than the detention of terrorists. If the courts are involved in the long view, they need to recognize that the horizon may very well be a cliff with a 300 foot drop.

So far there has been no overall challenge to the constitutionality of the PATRIOT Act or its major provisions. Some federal courts have taken up issues relating to legal authorities granted by the PATRIOT Act, with interesting results. XXXXX [add list].

For certain, the Supreme Court has yet to reach any major PATRIOT Act issue. There appear to be no such cases on the Court's current docket. But there is time. Even the more extreme provisions are not due to sunset until 2005, and the rest of the PATRIOT Act is permanent. Federal courts will be dealing with this statute indefinitely. Federal courts not only need to seriously take up the question of judicial oversight but also take it up in dramatic and effective ways for the protection of all Americans and all within her shores.

> 3. PATRIOT Act backlash. Perhaps some impetus for the strength that the judiciary needs to apply to its review of the PATRIOT Act and governmental conduct under its provisions, will come from the recent resolutions passed by several municipalities rejecting or criticizing the Act. Such resolutions were passed by towns in Massachusetts, California, and Colorado.

While these resolutions have no ultimate legal authority--the PATRIOT Act as a federal statute would override any such local government resolutions--their effect is to demonstrate to the federal government and to the citizenry nationwide that not all Americans will be as complacent as Congress and the White House might expect when it comes to the PATRIOT Act. If any trend identified in this series needs to continue, it is this. More municipalities and other jurisdictions small and large need to take notice of the issues and trends surrounding the PATRIOT Act and make it plain that they will not lie down and let the Constitution be sacrificed to the ever-expanding "war on terrorism."

> 4. Sunset provisions. Finally and perhaps most important, the American public cannot be distracted and complacent when it comes to those portions of the PATRIOT Act which are due to sunset. Certain sections in Title II are due automatically to sunset on December 31, 2005. The entire Title III is due to sunset on or before October 1, 2005 but only if Congress passes a joint resolution so declaring.

It stands to reason that if the American public remains complacent and if Congress continues to be distracted, pressure will be brought to bear--chiefly by federal investigative and intelligence agencies which have become far too accustomed their expanded surveillance, investigative, and prosecutorial powers--to repeal the sunset provisions for Title II and not to pass the joint resolution to inactivate Title III. That should not be allowed to happen, and only a vigilant American public can prevent it.

Of course, the Act does not explain what will happen to all of the information gathered, new federal offices established, and other activities initiated, under Titles II and III if these Titles do sunset. It is extremely doubtful that those offices will be disbanded or the information discarded. This in itself will be another matter to watch and another question to ask, as 2005 comes around.

C. William Michaels is an attorney and writer in Baltimore, Maryland. His just released book, No Greater Threat: America After September 11 and the Rise of a National Security State (Algora Publishing NYC, 2002) contains a review and analysis of the entire USA PATRIOT Act. The book is available from Barnes & Noble and Amazon.com. For more about the book and the author, go to "www.nogreaterthreat.com"

*In preparing these articles, Mr. Michaels gratefully acknowledges the assistance and collaboration of truthout.org columnist Jennifer Van Bergen (J.D. Cardozo School of Law; Faculty, New School University in New York).

Also see :

The Usa Patriot Act: One Year Later -- Part I | by C. William Michaels and Jennifer Van Bergen

The Usa Patriot Act: One Year Later -- Part II | by C. William Michaels

Free Speech & G.W. Bush | by Jennifer Van Bergen

Repeal the USA Patriot Act | by Jennifer Van Bergen

©: *t r u t h o u t 2002*

The Usa Patriot Act: One Year Later
Part I
by C. William Michaels and Jennifer Van Bergen
truthout | Report

Thursday, 14 November, 2002

On October 26 America observed a dubious anniversary--one year from the signing by President George W. Bush of the USA PATRIOT Act. The year has been an eventful one for all those concerned about the direction of the country and about civil liberties. Unfortunately, it also has a been a year when those who have followed developments since the PATRIOT Act have seen the formation of trends which, left unchecked, may fulfill the most dire predictions of those who have taken a long look at this comprehensive statute.

Among those predictions are the relative absence of judicial review of the Act, the bold movement by federal investigative and law enforcement agencies to utilize the substantial powers granted to them by the Act, the distraction of Congress on other matters muting Congressional oversight of these governmental agencies activities, and the complacency of large segments of the American public. The combination does not bode well for civil liberties or the national direction, especially given that the vast majority of the PATRIOT Act is permanent.

A Review of the Act and Themes

The USA PATRIOT Act stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." It was enacted by Congress virtually without significant debate, without detailed committee reports, without a conference committee, and with little floor commentary. Submitted just several days after the September 11 (2001) attacks, it was rushed through Congress at lightning speed for a statute of its size and complexity. It passed the House on October 24, 2001 by a vote of 357 to 66, and passed the Senate the next day, October 25, 2002, by a vote of 98 to 1. It was signed into law by President Bush the following day, October 26, and is now the law of the land.

The PATRIOT Act contains more than 150 sections. It is divided into ten separate Titles and is hundreds of pages long. The powers it grants to federal investigative agencies are unprecedented and reach everything from voice mail to consumer reports to banking records. It is highly doubtful that a statute as extensive as this could have been written from scratch while at the same time moving through Congress in a mere 45 days. Consider that the Homeland Security Act, considerably less extensive than the PATRIOT Act, is still bogged down in Congress after months, in limbo due to wrangling between the White House and the Senate over certain aspects such as internal structure and employee protections. The PATRIOT Act received no such attention yet its effects are tremendously more wide ranging.

Numerous activists groups such as ACLU, Center for Constitutional Rights, and others, sounded the alarm about the Act soon after it was introduced. However, the sea change in political climate which occurred virtually overnight after the September 11 attacks made the Act virtually unstoppable. Congress was determined to send a message to the terrorists and to give the White House what it wanted. The real question is what message ultimate will be sent and to whom. And it has become quite apparent that what the White House wanted by way of the PATRIOT Act is not necessary to effectively deal with the causes and incidents of terrorism. In fact, to date, no person has been arrested in the United States and charged with direct involvement in the September 11 attacks.

There was little to be done except watch as Congress enacted this monstrous statute. The American people will now be living with it for years to come.

Many misconceptions have arisen about the PATRIOT Act: it will sunset in a few years, the granted only limited authorities to federal agencies, it deals only with aliens or foreign nationals, and it is restrictive in length and scope. That is not so. The situation is far worse. Only very selected portions of the Act will sunset in 2005, the authorities it grants are massive, its reach conceivably can include every American,

and it contains extremely extensive and detailed provisions.

Of course, since September 11 there have been many other related developments: the military tribunals, the Office of Homeland Security, bioterrorism legislation, the new wave of aviation security, the globalization of the "war on terrorism," dramatic increases in surveillance of the public, skyrocketing military spending, the war in Afghanistan, and impending war with Iraq. Discussion of those would take us too far afield for present purposes since these developments have occurred parallel to but do not arise directly from the PATRIOT Act.

That does not leave us wanting. There is still plenty to review. The Act is among the most wide-ranging laws passed by Congress in recent memory, bringing new federal offices into being, creating new crimes, amending--in many cases substantially--at least 12 federal statutes, mandating dozens of new reports and regulations from agencies in four Cabinet Departments, and directly appropriating $2.6 billion (with more funding to come from approval of various "authorizations" of unnamed amounts, scattered throughout the statute).

At the outset, it may be worthwhile to list the Act's ten Titles, as a way of noting its grand scope:

Title I: Enhancing Domestic Security Against Terrorism

Title II: Enhanced Surveillance Procedures

Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (which has three subtitles and is by far the longest Title, representing the bulk of the Act's language)

Title IV: Protecting the Border

Title V: Removing Obstacles to Investigating Terrorism

Title VI: Providing for Victims of Terrorism, Public Safety Officers, and Their Families

Title VII: Increased Information Sharing for Critical Infrastructure Protection

Title VIII: Strengthening the Criminal Laws Against Terrorism

Title IX: Improved Surveillance

Title X: Miscellaneous

Going through these Titles and their sections, several themes appear consistently. Among them are: expansion of existing law, information sharing between federal investigative agencies, greater abilities for federal investigators to collect and utilize information, vigorous use of existing definitions of "foreign intelligence" and "terrorism," targeting of aliens as suspect groups, greatly increased surveillance and prosecutorial powers, enhanced visibility and responsibility of the entire intelligence community, and limited judicial review. These themes certainly have marked the use of Act's powers by federal agencies in the past year.

A Tour Through Act Highlights

It is not possible in this limited space to describe each of the Act's ten Titles, although just a review of the title names themselves provides a sense of how extensive the PATRIOT Act is. Unfortunately, most of the attention paid to the Act in the general media and by most activist groups has been devoted to Title II and Title VI, which means eight of its Titles have received relatively little comment. Without getting too involved, a brief tour through some of the Act's highlights will underscore concerns raised so far and point out areas that to date have been effectively overlooked:

Section 101--Establishes a new counterterrorism fund without fiscal year limitation and of unnamed amount, to be administered by the Justice Department for its own use.

Section 103--Re-invigorates the Justice Department's "Technical Support Center" (established by the Anti Terrorism and Effective Death Penalty Act of 1996) and gives it $200 million for each of the next three years, 2002 through 2004.

Section 105: Establishes a "national network of electronic crimes task forces" to be set up by the Secret Service throughout the country to prevent, detect, and investigate various electronic crimes "including potential terrorist attacks against critical infrastructures and financial payment systems"--which can mean a wide variety of computer crimes.

Section 203: Mandates information sharing, including of previously secret grand jury testimony, between any number of federal agencies so long as the information involves "foreign intelligence"--using the broad definition of that term found in the Foreign Intelligence Surveillance Act (FISA), a definition which includes the following: "information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to the national defense or the security of the United States or the conduct of the foreign affairs of the United States." Such information which is in the possession of any federal investigative or law enforcement officer or attorney can be shared--without any court review or involvement--with any other federal "law enforcement, intelligence, protective, immigration, national defense, or national security official."

Section 218: Changes the scope of warrants under FISA from foreign intelligence being "a purpose" to "a significant purpose" of the investigation and so lowers the standard for obtaining a FISA warrant (assuming such warrants were difficult to obtain in the past and that most definitely has not been the case). Note that an investigation under FISA even though it usually involves foreign nationals or aliens does not have to be so restricted, and under the broad definition of "foreign intelligence" can include United States citizens.

Sections 207 and 208: Increases the duration of FISA warrants and boosts the number of FISA court judges.

Section 209, 212, 215, 216: Sets into motion numerous technical changes and enhancements for standard surveillance techniques, for example, taking voice mail out of the requirements of wiretap statutes, and authorizing the use of "Carnivore" type electronic computer surveillance programs.

Section 212: Provides for voluntary and required disclosures to federal investigators by firms such as Internet service providers.

Section 213: Allows delayed notification of "non-physical search and search warrants" (known as sneak and peek warrants) generally used in FISA investigations but could be used in other investigations.

Section 215: Allows access to "any tangible thing" for federal investigators in FISA-type investigations.

Section 219/220: Sets up single jurisdiction search warrants and nationwide service of warrants.

Section 311: A highly technical section allowing for federal investigators, in certain conditions, to impose extreme "special measures" upon any domestic bank or financial institution, seeking information related to terrorist financing.

Section 312: Another detailed provision imposing upon banks and domestic financial

entities new "minimal" and "enhanced" due diligence requirements on certain accounts, as a way of revealing possible use of accounts for terrorist financing (exhaustive Treasury regulations and other directives already have been issued on the requirements of Sections 311 and 312).

Section 319: Sets a 120-hour deadline for financial institutions to respond to certain information requests by federal investigators involving wide range of accounts.

Section 316 and 319: Creates new forfeiture provisions for those charged or convicted of certain terrorist crimes especially including money laundering, setting forfeiture authorities virtually unheard of in federal law to this point.

Section 319: Permits access by federal investigators of records of certain "correspondent" accounts with foreign banks.

Section 326: Establishes new or expanded requirements to track identities of persons opening new bank accounts.

Section 326: Authorizes a study to track aliens or foreign nationals by a system similar to social security numbers.

Section 358: Allows government investigator access to consumer records, which does not require a court order and is to be provided in secret and without civil liability.

Section 361: Establishes or expands the "FinCEN" office in the Treasury Department, accompanied by a long list of duties for this office and substantial funding.

Section 403: Mandates a dramatic new information system to allow State Department access to certain criminal files kept by the FBI (such as NCIC-III files).

Section 403: Requires a new technology standard to be applied to visas and all border checkpoints, including biometric methods.

Section 414-417: Sets up new standards and studies for entry and exist systems and data systems for border entry points, including machine-readable passports.

Section 411: Creates a new definition of terrorism for this Title, notably establishing three separate types of "terrorist organization" with wide latitude by federal investigations such as in the State Department to "identify" these terrorist groups.

Section 412: Provides for mandatory detention of suspected aliens, lists seven bases for such detention, allows for a person to be held for seven days without any charge, permits possible indefinite detention for aliens deemed not removable, and ensures limited court review.

Section 412: Requires biannual report to Congress on aliens detained, but this report is not required to contain essential information such as name, when seized, where detained, or nature of charges.

Section 416: Expands, with increased funding, the foreign student monitoring program.

Section 503: Greatly expands the DNA information bank as to criminals, which now will include any crime of violence and all terrorist crimes.

Section 504: Links investigation of any crime with search for foreign intelligence, for purposes of information sharing.

Section 505: Allows government investigators access to consumer reports, without court order, also to be produced in secret and without civil liability.

Section 507 and 508: Allows government investigators access to educational records, without court order.

Section 701: Establishes a major initiative for a "secure information sharing system" to assist all law enforcement agencies, and this would include State and local agencies, to investigate and prosecute multi-jurisdictional terrorist conspiracies and activities.

Section 802: Creates new crime of "domestic terrorism."

Section 803: Expands or clarifies the crimes of harboring, concealing, or providing material support for terrorists.

Section 808: Expands the extensive list of "federal crime of terrorism" which now includes certain computer crimes.

Sections 809-812: Provides for no statute of limitations for certain terrorist crimes, and allows increased penalties--including "supervised release" similar to parole in federal system, which now can be up to life (unheard of in federal sentencing system until now).

Section 901: Mandates information sharing by CIA to Justice Department.

Section 903: An unusual Section which deputizes all "officers and employees" of the "intelligence community" (13 agencies) and turns them into mini-CIA to investigate terrorism.

Section 905: Mandates information sharing by Justice Department and similar law enforcement agencies to CIA.

Section 908: Sets up an ongoing cross agency training program for various law enforcement officials and agencies, including State and local, so they can better recognize "foreign intelligence" material, information, or evidence in their criminal surveillance or investigations.

Section 1005: Provides grants for State and local fire and emergency response departments, under the "First Responders Assistance Act," which grants can include technology and equipment for intelligence gathering and analysis, and funds the program at $25 million for fiscal years 2003 through 2007.

Section 1016: Establishes new programs for critical infrastructure protection.

The Record So Far

With these greatly expanded powers, covering a long list of new authorities and mandates, federal agencies have been busy. In the Justice Department, information sharing protocols authorized by the PATRIOT Act were recently issued by Attorney General John Ashcroft. These protocols make it clear that the Justice Department will use to the fullest extent, the authorities granted to it by the Act. Among this information sharing is communication by Justice Department personnel to intelligence personnel within 30 days on whether a criminal investigation will be launched based on a given crime report, if the crime report indicates that foreign intelligence may be involved. New FBI guidelines on undercover operations have been announced which roll back permitted FBI activity to a activities of nearly 30 years ago that were the subject of widespread criticism.

New federal investigative task forces are being created, with Justice Department in the lead, including identification by the United States Attorney for each judicial district of members of a terrorist task force

which can be quickly assembled from local federal agency personnel when the need arises. Also, there are several ongoing cross agency task forces to investigate terrorism or terrorist financing such as Operation Green Quest.

The Treasury Department has issued tremendously detailed regulations for Title III's new requirements for banks and other financial institutions. Title III has effectively rewritten many banking laws and introduced new requirements to the point that domestic bank are virtual partners with the federal government in investigating financial aspects of terrorism. Spurred by PATRIOT Act authority to investigate any forms of money transfer that may be linked to terrorism, new arrests and detentions have been made by federal agents of principals of certain targeted charitable groups which send money abroad, especially to the Middle East, shutting these organizations down under the guise of investigating terrorism.

The State Department, on its own or through Executive Order, has identified a whole new list of terrorist groups. Cooperating with the INS, FBI and in some instances CIA, information sharing has gotten to the point where a suspected terrorists can be arrested or rounded up by any number of these agencies. The State Department has cooperated with the INS (in the Justice Department) to round up thousands of aliens suspected of terrorism, although most have been either released, given minor charges, deported on visa or other technical violations. In August, 2002, a federal court (Judge Gladys Kessler) ruling in favor of various groups who sued the Justice Department and the INS demanding information on detainees, recently ordered the government to release the names of the remaining detainees (as many as 150). But the government has refused to do so citing national security concerns and has sought a stay of the order pending appeal.

The PATRIOT Act has given not only new authorities but also a new hubris to federal investigative agencies. Its emphases on information collection, information sharing, expanded definitions, new regulations, cross-agency cooperation, wider authorities, enhanced surveillance techniques, swifter prosecutions, and more severe sentences have brought law enforcement and terrorism investigation in America to new levels. Unfortunately, Congress, having handed over such tremendous authorities to the Executive Branch, has spent little time reviewing what it has wrought. But the PATRIOT Act cannot fade into the distance. It is very much with us, and its effects have not yet totally been felt.

Although many watchdog groups and organizations are turning their attention to other things, we cannot totally turn our backs on these developments. The second Part of this two part article will take a look at some emerging trends and note items for special attention in the foreseeable future.

C. William Michaels is an attorney and writer in Baltimore, Maryland. His just released book, No Greater Threat: America After September 11 and the Rise of a National Security State (Algora Publishing NYC, 2002) contains a review and analysis of the entire USA PATRIOT Act. The book is available from Barnes & Noble and Amazon.com. For more about the book and the author, go to www.nogreaterthreat.com

Jennifer Van Bergen is a graduate of Cardozo School of Law in NY and is on the faculty of the New School University in New York. Her six part article series for "truthout" "Repeat the PATRIOT Act" in April-June 2002 was one of the first widely distributed and detailed public commentaries on the statute. She is a columnist for truthout.

Also see :

The Usa Patriot Act: One Year Later -- Part I | by C. William Michaels and Jennifer Van Bergen

The Usa Patriot Act: One Year Later -- Part II | by C. William Michaels

This Document did not include a Page 7 of 7

Rep. Almy, Graf 18
Rep. Kurk, Hills 48
Rep. Hatch, Carr 7
Rep. Buhlman, Hills 66
May 6, 2003
2003-1515h
05/01

Amendment to HCR 9

Amend the resolution by replacing the title of the resolution with the following:

A RESOLUTION urging the United States Congress to ensure the constitutionality of the implementation of the Total Information Awareness Program, the USA PATRIOT ACT, and any successors.

Amend the resolution by replacing all after the title with the following:

Whereas, our nation and our state were founded to escape and prevent tyranny by the establishment of multiple checks upon the power of our respective governments, and by the careful restraint of executive and military power over our civilian population; and

Whereas, the Department of Defense of the United States of America has been exploring a program named Total Information Awareness which would attempt to requisition and correlate every existing private and public database on our nation's individual citizens and residents; and

Whereas, these databases are said to include those of credit records, employment histories, gun registries, divorce, medical, and educational records, drivers' licenses, catalog purchases, civil lawsuits, criminal proceedings, Social Security information, professional licenses, passport applications, civil and military service dossiers, bank accounts, computerized road toll records, IRS records, insurance records, savings and debt transactions, airline travel, FBI and police dossiers, video and cable viewing records, surveillance cameras, computer activity records, and library records; and

Whereas, this degree of government knowledge of the lives of ordinary Americans, and potential control of their individual data, could be devastating to our liberty and our Republic, if ever used for personal or political gain by individual government employees, or by a future Commander in Chief or agency head for control of legitimate domestic dissent, political activity, key economic actors or the media; and

Whereas, even under the assumption that no future office-holder would be tempted by the illegitimate abuse of this vast power over the citizenry, the temptation to extend its use into the civilian concerns of ordinary crime would be difficult to resist, and effectively abolish all Constitutional guarantees against government searches and seizures; and

Whereas, the United States Congress has recently established budgetary controls to require strict accounting from the Department of Defense of constitutional and legal privacy concerns before the Total Information Awareness program is allowed to proceed; but

Whereas, on October 24, 2001, in the shadow of the atrocious acts occurring on September 11, 2001, the United States Congress, before applying its usual careful consideration, passed the USA PATRIOT ACT, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; and

Whereas, this act has made it legal for government agents to enter and search a citizen's home, or obtain an individual's or a class of citizens' medical, bank, credit, business, library, and other records, using a warrant issued by a secret court that is barred by the act from refusing the government's request, and withholding from those citizens and the public the knowledge that the search and seizures have occurred; and

Whereas, these powers can be used in investigations having nothing to do with terrorism, requiring only an agent's allegation that the investigation may touch on terrorism; and

Whereas, the existing war on terrorism is not a war in the traditional sense of the term, but a state of alertness without an end limit, and therefore could be used to justify the permanent destruction of our cherished liberties and way of life unless appropriate action is taken; and

Whereas, the USA PATRIOT ACT defines the new crime of domestic terrorism in such a way that many if not most advocacy groups in this nation could qualify as terrorist, if the Attorney General of the United States so chooses; and

Whereas, the government is reportedly planning an expansion of these powers, called the Domestic Security Enhancement Act of 2003, which defines domestic crimes for which an American citizen could be stripped of citizenship; and

Whereas, the Attorney General is granted the power to remove many of the checks and balances that have preserved our liberty and our security for more than 220 years, and particularly those of judicial and public scrutiny; now, therefore, be it

Resolved by the New Hampshire House of Representatives, the Senate concurring:

That the Congress of the United States of America is to be commended for its actions to date in protecting our cherished liberties relative to the Total Information Awareness program; and

That the United States Congress is strongly urged to undertake an investigation of the USA PATRIOT ACT to determine how it has been used, and to repeal or amend any provisions that have resulted in undue infringements on the legal activities of the citizens and residents of this great country, thereby restoring confidence in the protections guaranteed under the Bill of Rights; and

That the United States Congress is urged to prevent the further expansion of these intrusive government powers by refusing to consider the Domestic Security Enhancement Act unless it is amended to respect all the guarantees of the Bill of Rights; and

That copies of this resolution be forwarded by the house clerk to the President of the United States, the Attorney General, the Joint Chiefs of Staff in Arlington, Virginia, and each member of the New Hampshire congressional delegation.

2003-1515h

AMENDED ANALYSIS

This resolution urges the United States Congress to ensure the constitutionality of the implementations of the Total Information Awareness Program, the USA PATRIOT ACT, and any successors.

Speakers

SENATE INTERSTATE COOPERATION COMMITTEE

Date 45/7/03 Time 3:15 p.m. Public Hearing on HCR 9

HCR 9 - urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

(Insert here the title of the Bill)

Please check box(es) that apply.

SPEAKING	FAVOR	OPPOSED	NAME (Please print)	REPRESENTING
☒	☒	☐	Rep Almy	
☒	☒	☐	Rep. M. Smith	
☒	☒	☐	Rep. Kurk	
☒	☒	☐	Claire Ebel	NHCLU
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		
☐	☐	☐		

Testimony

ELECTRONIC PRIVACY INFORMATION CENTER

Total Information Awareness (TIA)

Introduction | News | Resources

Introduction

The Total Information Awareness project is part of the Defense Advanced Research Projects Agency's Information Awareness Office. The office is headed by Admiral (retired) John Poindexter who is responsible for conceiving the project. TIA purports to capture the "information signature" of people so that the government can track potential terrorists and criminals involved in "low-intensity/low-density" forms of warfare and crime. The goal is to track individuals through collecting as much information about them as possible and using computer algorithms and human analysis to detect potential activity.

The project calls for the development of "revolutionary technology for ultra-large all-source information repositories," which would contain information from multiple sources to create a "virtual, centralized, grand database." This database would be populated by transaction data contained in current databases such as financial records, medical records, communication records, and travel records as well as new sources of information. Also fed into the database would be intelligence data.

A key component of the TIA project is to develop data-mining or knowledge discovery tools that will sort through the massive amounts of information to find patterns and associations. TIA will also develop search tools such as Project Genoa, which Admiral Poindexter's former employer Syntek Technologies, assisted in developing. TIA aims to fund the development of more such tools and data-mining technology to help analysts understand and even "preempt" future action.

A further crucial component is the development of biometric technology to enable the identification and tracking of individuals. DARPA has already funded its "Human ID at a Distance" program, which aims to positively identify people from a distance through technologies such as face recognition or gait recognition. A nationwide identification system would be of great assistance to such a project by providing an easy means to track individuals across multiple information sources.

DARPA's Broad Agency Announcement 02-08 soliciting proposals from industry states that the initial plan is for a five year research project into these various technologies. The interim goal is to build "leave-behind prototypes with a limited number of proof-of-concept demonstrations in extremely high risk, high payoff areas." The FBI and the Transportation Security Administration are also working on data-mining projects that will fuse commercial databases, public databases, and intelligence data and had meetings with TIA developers.

WILLIAM SAFIRE

You Are a Suspect

WASHINGTON

If the Homeland Security Act is not amended before passage, here is what will happen to you:

Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade your receive, every bank deposit you make, every trip you book and every event you attend — all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database."

To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you — passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the latest hidden camera surveillance — and you have the supersnoop's dream: a "Total Information Awareness" about every U.S. citizen.

This is not some far-out Orwellian scenario. It is what will happen to your personal freedom in the next few weeks if John Poindexter gets the unprecedented power he seeks.

Remember Poindexter? Brilliant man, first in his class at the Naval Academy, later earned a doctorate in physics, rose to national security adviser under President Ronald Reagan. He had this brilliant idea of secretly selling missiles to Iran to pay ransom for hostages, and with the illicit proceeds to illegally support contras in Nicaragua.

A jury convicted Poindexter in 1990 on five felony counts of misleading Congress and making false statements, but an appeals court overturned the verdict because Congress had given him immunity for his testimony. He famously asserted, "The buck stops here," arguing that the White House staff, and not the president, was responsible for fateful decisions that might prove embarrassing.

This ring-knocking master of deceit is back again with a plan even more scandalous than Iran-contra. He heads the "Information Awareness Office" in the otherwise excellent Defense Advanced Research Projects Agency, which spawned the Internet and stealth aircraft technology. Poindexter is now realizing his 20-year dream: getting the "data-mining" power to snoop on every public and private act of every American.

Even the hastily passed U.S.A. Patriot Act, which widened the scope of the Foreign Intelligence Surveillance Act and weakened 15 privacy laws, raised requirements for the government to report secret eavesdropping to Congress and the courts. But Poindexter's assault on individual privacy rides roughshod over such oversight.

He is determined to break down the wall between commercial snooping and secret government intrusion. The disgraced admiral dismisses such necessary differentiation as bureaucratic "stovepiping." And he has been given a $200 million budget to create computer dossiers on 300 million Americans.

When George W. Bush was running for president, he stood foursquare in defense of each person's medical, financial and communications privacy. But Poindexter, whose contempt for the restraints of oversight drew the Reagan administration into its most serious blunder, is still operating on the presumption that on such a sweeping theft of privacy rights, the buck ends with him and not with the president.

This time, however, he has been seizing power in the open. In the past week John Markoff of The Times, followed by Robert O'Harrow of The Washington Post, have revealed the extent of Poindexter's operation, but editorialists have not grasped its undermining of the Freedom of Information Act.

Political awareness can overcome "Total Information Awareness," the combined force of commercial and government snooping. In a similar overreach, Attorney General Ashcroft tried his Terrorism Information and Prevention System (TIPS), but public outrage at the use of gossips and postal workers as snoops caused the House to shoot it down. The Senate should now do the same to this other exploitation of fear.

The Latin motto over Poindexter's new Pentagon office reads "Scientia Est Potentia" — "knowledge is power." Exactly: the government's infinite knowledge about you is its power over you. "We're just as concerned as the next person with protecting privacy," this brilliant mind blandly assured The Post. A jury found he spoke falsely before. □

E-mail: safire@nytimes.com

Individual Liberty,
Limited Government,
Free Markets and Peace

Search
Advanced Search
Help

Terrorism
- Terrorism Home
- The Military Response
- The Diplomatic Response
- Civil Liberties
- Bioterror and Other Future Threats
- Economic Impact
- Political Impact
- America's Values under Attack
- Press Information

Contribute
- Make a Contribution
- About Sponsorship
- Alternative Giving Methods
- Levels and Benefits

Cato Offerings

The USA Patriot Act: We Deserve Better
by Robert A. Levy, Senior Fellow in Constitutional Studies, Cato Institute

A version of this article orginally appeared in *Liberty* magazine.

If you think the Bill of Rights is just so much scrap paper, and the separation of powers doctrine has outlived its usefulness, then the USA PATRIOT Act, passed overwhelmingly on Oct. 25, is the right recipe to deal with terrorists. On the other hand, if you are concerned about Fifth Amendment protection of due process, and Fourth Amendment safeguards against unreasonable searches and seizures, then you should be deeply troubled by the looming sacrifice of civil liberties at the altar of national security.

To be sure, the Constitution is not a suicide pact. Government is legitimately charged with defending life, liberty, and property against both domestic and foreign predators. First among those obligations is to protect life. With America under attack, and lives at risk, civil liberties cannot remain inviolable. But that's a far cry from asserting that they may be flouted to wage war against fanatics.

Proponents of the new bill surely understood that many of its provisions were incompatible with civil liberties. Yet rather than modify the offending provisions, the president and Congress decided to promote the bill as an expression of patriotism. Hence the acronym - USA PATRIOT - and its bloated title, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The sales pitch worked. Fearful of being labeled disloyal after the September atrocities, the House endorsed the bill 357-to-66, followed by a 98-to-1 rout in the Senate, with only Russ Feingold (D-Wis.) in opposition.

From its initial draft to its final adoption, USA PATRIOT zipped through in six weeks - gutting much of the Fourth Amendment in far less time than Congress typically expends on routine bills that raise no constitutional concerns. Congress' so-called deliberative process was reduced to this: Closed-door negotiations; no conference committee; no committee reports; no final hearing at which opponents could testify; not even an opportunity for most of the legislators to read the 131 single-spaced pages about to become law. Indeed, for part of the time, both the House

May 6, 2003
Daily Commentary
Homeland Security: Follow the Bouncing Ball

by Charles V. Peña

Minority Rules: Filibustering the Constitution

by James L. Swanson

[Archives]

Daily Dispatch
- Bush Trying to Stop North Korea from Exporting Nuclear Material
- New Legislation Would Protect Gun Industry From Lawsuits
- Pakistan Will Disarm Nukes if India Does

[Archives]

Over This Week
May 7, 2003
The Real Environmental Crisis: Why Poverty, Not Affluence, Is the Environment's Number One Enemy
11:00 a.m.
Cato Book Forum

Subscribe to Updates

The USA Patriot Act: We Deserve Better

by Robert A. Levy, Senior Fellow in Constitutional Studies, Cato Institute

A version of this article orginally appeared in *Liberty* magazine.

If you think the Bill of Rights is just so much scrap paper, and the separation of powers doctrine has outlived its usefulness, then the USA PATRIOT Act, passed overwhelmingly on Oct. 25, is the right recipe to deal with terrorists. On the other hand, if you are concerned about Fifth Amendment protection of due process, and Fourth Amendment safeguards against unreasonable searches and seizures, then you should be deeply troubled by the looming sacrifice of civil liberties at the altar of national security.

To be sure, the Constitution is not a suicide pact. Government is legitimately charged with defending life, liberty, and property against both domestic and foreign predators. First among those obligations is to protect life. With America under attack, and lives at risk, civil liberties cannot remain inviolable. But that's a far cry from asserting that they may be flouted to wage war against fanatics.

Proponents of the new bill surely understood that many of its provisions were incompatible with civil liberties. Yet rather than modify the offending provisions, the president and Congress decided to promote the bill as an expression of patriotism. Hence the acronym - USA PATRIOT - and its bloated title, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. The sales pitch worked. Fearful of being labeled disloyal after the September atrocities, the House endorsed the bill 357-to-66, followed by a 98-to-1 rout in the Senate, with only Russ Feingold (D-Wis.) in opposition.

From its initial draft to its final adoption, USA PATRIOT zipped through in six weeks - gutting much of the Fourth Amendment in far less time than Congress typically expends on routine bills that raise no constitutional concerns. Congress' so-called deliberative process was reduced to this: Closed-door negotiations; no conference committee; no committee reports; no final hearing at which opponents could testify; not even an opportunity for most of the legislators to read the 131 single-spaced pages about to become law. Indeed, for part of the time, both the House and Senate were closed because of the anthrax scare; congressional staffers weren't able to access their working papers.

The negligible legislative record will make it difficult for courts to determine the intent of Congress. And because legislative intent matters to some judges - for example, Supreme Court Justices Stephen Breyer and David Souter - the USA PATRIOT statute might ultimately be invalidated as unconstitutionally vague. Ironically, Congress' rush job, which facilitated passage of the bill, could be the cause of the bill's downfall. The same law that was promoted as an act of patriotism might even provide a rationale for releasing the madmen who committed the horrific terrorist acts against the United States.

Yet the more acute objections to the new statute are substantive, not procedural. They fall into three main categories. First, any law with the potential to dramatically alter conventional notions of individual freedom should fastidiously guard against abuse. The doctrine of separation of powers, a centerpiece of our Constitution, has been a traditional buffer against such abuse. By requiring advance judicial authorization of certain executive actions, followed by judicial review to assure that those actions have been properly performed, our liberties are shielded from excessive concentrations of power in a single branch of government. As we shall see, the USA PATRIOT Act does not pass muster.

Second, if the new rules are at all justifiable, they are defended as a necessary instrument of anti-terrorism. If so, why do many of the provisions apply not only to suspected terrorist acts but also to everyday national security investigations and even ordinary criminal matters? In effect, our government has exploited the events of Sept. 11 to impose national police powers that skirt time-honored constraints on the state. The executive branch will not always wield its new powers in the service of ends that Americans find congenial. Better that the government be shackled by the chains of the Constitution.

Third, laws that compromise civil liberties must be revisited periodically to assure that temporary measures, undertaken in response to a national security emergency, do not endure longer than necessary. Such laws must contain sunset clauses; that is, the law should expire automatically within a short time of enactment - thus imposing on government the continuing obligation to justify its intrusions. In this instance, the Bush Administration rejected any sunset provision whatsoever. Congress demurred, and insisted on including such a provision; but it applied only to new wiretap and surveillance powers, not to the whole bill. Moreover, the sunset date was fixed at Dec. 31, 2005 - more than four years after passage of the legislation. Plainly, a shorter time frame - one year, or two years at most - would have been appropriate. If the emergency persisted, Congress and the president could reenact the law.

Skeptics might dismiss those objections as mere abstractions - civil libertarianism run amok - unless they are illuminated by concrete examples from the statute. Here, then, are just a few of the more egregious threats to personal freedom.

During the Carter administration, Congress passed the Foreign Intelligence Surveillance Act, which created a new federal court to approve electronic surveillance of citizens and resident aliens alleged to be acting on behalf of a foreign power. Until now, the FISA court granted surveillance authority if foreign intelligence was the primary purpose of an investigation. No longer. Under Section 218 of the USA PATRIOT Act, foreign intelligence need only be "a significant purpose" of an investigation. That sounds like a trivial change, but it isn't. Because the standard for FISA approval is lower than "probable cause," and because FISA now applies to ordinary criminal matters if they are dressed up as national security inquiries, the new rules could open the door to circumvention of the Fourth Amendment's warrant requirements. The result: rubber-stamp judicial supervision of phone and Internet surveillance, even in regular criminal cases, and FBI access to medical, educational, and other business records that might conceivably relate to foreign intelligence probes.

The FISA revision is but one example of the government's expanded powers to conduct searches and surveillance. There are others. Government will have access to some financial records, without notice or judicial review. While judicial approval is necessary to retrieve voicemail messages, the requisite court order can now be obtained with a minimal showing of relevancy. That same low standard governs traces on Internet surfing and email. Perhaps worst of all, under Section 213 of the Act, secret "sneak and peek" searches of physical property will be condoned in routine criminal investigations. Those searches can be conducted without knowledge of the property owner until a "reasonable" time after the search has occurred. No knowledge means no opportunity to contest the validity of the search, including such obvious infractions as rummaging through office drawers when the warrant authorizes a garage search, or even searching the wrong address.

On the money laundering front (Sections 301 through 377), the secretary of the treasury is empowered to label any jurisdiction a "primary money laundering concern," in which case foreign banks will be required to disclose their customers and transactions. Predictably, the identified countries will be those with low tax structures and strict financial privacy laws. Yet there is little evidence that tax havens are

a magnet for dirty money. In fact, when money is transferred across borders and back again, the risk of detection is high. That serves as a deterrent to such transactions. To punish nations that harbor terrorists and their assets, we should shut off U.S. access to financial institutions that refuse to provide evidence associated with the September carnage. We should also invoke existing bilateral agreements, and negotiate new agreements, waiving bank secrecy and requiring mutual cooperation when prosecuting terrorist acts.

Finally, civil libertarians are rightly alarmed that the attorney general can detain, for seven days, non-citizens suspected of terrorism. After seven days, pursuant to Section 412 of the Act, deportation proceedings must commence or criminal charges must be filed. Originally, the Justice Department had asked for authority to detain suspects indefinitely without charge. Congress could not be persuaded to go along. But the final bill, for all practical purposes, allows expanded detention simply by charging the detainee with a technical immigration violation. And if a suspect cannot be deported, he can still be detained if the attorney general certifies every six months that national security is at stake.

To illustrate the magnitude and scope of that problem, the *Wall Street Journal* reported on Nov. 1 that seven Democrats had filed Freedom of Information Act requests for a detailed accounting from Attorney General John Ashcroft on the status of more than 1,000 detainees. The lawmakers cited reports that "some detainees have been denied access to their attorneys, proper food, or protection from ... physical assault." Some of them were allegedly being held in solitary confinement even though they hadn't been charged with any criminal offense. According to a representative of the New York Legal Aid Society, several Arab detainees had been limited to one phone call per week to a lawyer and, if the line was busy, they had to wait another week.

Maybe those reports will turn out to be groundless. But it's time for some answers. Here's what the *Washington Post* had to say in an Oct. 31 editorial: "The Department of Justice continues to resist legitimate requests for information regarding the 1,017 people it acknowledges having detained in its investigation of the September 11 attacks.... The questions are pretty basic. How many of the 1,000-plus are still in custody? Who are they? What are the charges against them? What is the status of their cases? Where and under what circumstances are they being held? The department refuses not only to provide the answers but also to give a serious explanation of why it won't provide them."

Ultimately, the Supreme Court may have to clarify how the civil liberties / national security tradeoff will unfold. This past term, in *Zadvydas v. Underdown*, the Court held that immigrants who have committed crimes cannot be detained indefinitely, but must be deported within a reasonable period or released. Moreover, said the Court, temporary and even illegal immigrants, not just U.S. citizens, are entitled to due process. Still, the Court noted that different rules may apply to immigrants who are denied entry, suspected of terrorism, or considered to be national security risks.

Thus, the law is murky; and the legislation passed in the aftermath of September's events adds new elements of uncertainty. Nonetheless, the controlling principle is unambiguous. Any attempt by government to chip away at constitutionally guaranteed rights must be subjected to the most painstaking scrutiny to determine whether less invasive means could accomplish the same ends. The USA-PATRIOT anti-terrorism bill does not survive that demanding test. In a free society, we deserve better.

USAPATRIOT

SEC. 802. DEFINITION OF DOMESTIC TERRORISM.

(a) DOMESTIC TERRORISM DEFINED- Section 2331 of title 18, United States Code, is amended--

(1) in paragraph (1)(B)(iii), by striking `by assassination or kidnapping' and inserting `by mass destruction, assassination, or kidnapping';

(2) in paragraph (3), by striking `and';

(3) in paragraph (4), by striking the period at the end and inserting `; and'; and

(4) by adding at the end the following:

`(5) the term `domestic terrorism' means activities that--

`(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

`(B) appear to be intended--

`(i) to intimidate or coerce a civilian population;

`(ii) to influence the policy of a government by intimidation or coercion; or

`(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

`(C) occur primarily within the territorial jurisdiction of the United States.'.

if you or your legal partner sends dues to an organization so defined, you are liable

organizations or acts that could qualify:

- PETA
- the tree-sitters in the North West
- Operation Rescue
- motorcycle groups
- militias
- any public demonstration during which a few trouble-makers set off a coercive police response
- strike actions ditto

SEC. 507. DISCLOSURE OF EDUCATIONAL RECORDS.

Section 444 of the General Education Provisions Act (20 U.S.C. 1232g), is amended by adding after subsection (i) a new subsection (j) to read as follows:

`(j) INVESTIGATION AND PROSECUTION OF TERRORISM-

`(1) IN GENERAL- Notwithstanding subsections (a) through (i) or any provision of State law, the Attorney General (or any Federal officer or employee, in a position not lower than an Assistant Attorney General, designated by the Attorney General) may submit a written application to a court of competent jurisdiction for an ex parte order requiring an educational agency or institution to permit the Attorney General (or his designee) to--

`(A) collect education records in the possession of the educational agency or institution that are relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of title 18 United States Code, or an act of domestic or international terrorism as defined in section 2331 of that title; and

`(B) for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such records, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.

`(2) APPLICATION AND APPROVAL-

`(A) IN GENERAL- An application under paragraph (1) shall certify that there are specific and articulable facts giving reason to believe that the education records are likely to contain information described in paragraph (1)(A).

`(B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).

`(3) PROTECTION OF EDUCATIONAL AGENCY OR INSTITUTION- An educational agency or institution that, in good faith, produces education records in accordance with an order issued under this subsection shall not be liable to any person for that production.

`(4) RECORD-KEEPING- Subsection (b)(4) does not apply to education records subject to a court order under this subsection.'.

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';

(2) by inserting `, routing, addressing,' after `dialing'; and

(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

`(a) IN GENERAL-

`(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

`SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

`(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

`(2) An investigation conducted under this section shall--

`(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

`(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

`(b) Each application under this section--

`(1) shall be made to--

`(A) a judge of the court established by section 103(a); or

`(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

`(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

`(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

`(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

SEC. 508. DISCLOSURE OF INFORMATION FROM NCES SURVEYS.

Section 408 of the National Education Statistics Act of 1994 (20 U.S.C. 9007), is amended by adding after subsection (b) a new subsection (c) to read as follows:

'(c) INVESTIGATION AND PROSECUTION OF TERRORISM-

'(1) IN GENERAL- Notwithstanding subsections (a) and (b), the Attorney General (or any Federal officer or employee, in a position not lower than an Assistant Attorney General, designated by the Attorney General) may submit a written application to a court of competent jurisdiction for an ex parte order requiring the Secretary to permit the Attorney General (or his designee) to--

'(A) collect reports, records, and information (including individually identifiable information) in the possession of the center that are relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of title 18, United States Code, or an act of domestic or international terrorism as defined

'(B) for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such information, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.

'(2) APPLICATION AND APPROVAL-

'(A) IN GENERAL- An application under paragraph (1) shall certify that there are specific and articulable facts giving reason to believe that the information sought is described in paragraph (1)(A).

'(B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).

'(3) PROTECTION- An officer or employee of the Department who, in good faith, produces information in accordance with an order issued under this subsection does not violate subsection (b)(2) and shall not be liable to any person for that production.'.

'Sec. 626. Disclosures to governmental agencies for counterterrorism purposes

'(e) SAFE HARBOR- Notwithstanding any other provision of this title, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a governmental agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.'.

SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.

Section 3103a of title 18, United States Code, is amended--

(1) by inserting `(a) IN GENERAL- ' before `In addition'; and

(2) by adding at the end the following:

`(b) DELAY- With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if--

`(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);

`(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

`(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.'.

SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.

(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-

(1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:

'(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.'.

Search

Advanced Search
Help

Publications

- Books
- Policy Studies
- Cato Policy Report
- Cato Journal
- Regulation Magazine
- Cato Handbook for Congress
- Congressional Testimony
- Legal Briefs
- Cato Audio
- Cato's Letters
- To Be Governed...
- Events Archive

25th Anniversary

- 25th Home
- Friedman Prize
- Milton Friedman
- About Cato
- Cato Timeline

Contribute

- Make a Contribution
- About Sponsorship
- Alternative Giving Methods
- Levels and Benefits

Cato Offerings

December 7, 2002

Total Information Awareness: Back to the Future

by Charles V. Peña

Charles V. Peña is senior defense policy analyst at the Cato Institute.

The idea of "total information awareness," or TIA, has come under fire lately. And for good reason. This new system for intelligence gathering could backfire and lead to a repetition of the intelligence failures America experienced prior to 9/11.

TIA is a Pentagon program designed to build a large-scale counter-terrorism database from myriad sources, including e-mail, electronic and credit card purchases, airline travel, rental cars, telephone calling cards, gun purchases, and medical records.

Supporters argue that it's an advanced computer tool intended to help catch would-be terrorists by looking for links and patterns indicative of terrorist activity. Critics are concerned that the TIA program would be the first step towards a surveillance state and allow the U.S. government to monitor and spy on its own citizens. For example, some critics have written the following:

- "[W]e do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?"

- "The administration's interest in e-mail is a wholly unhealthy precedent, especially given this administration's track record on FBI files and IRS snooping. Every medium by which people communicate can be subject to exploitation by those with illegal intentions. Nevertheless, this is no reason to hand Big Brother the keys to unlock our e-mail diaries, open our ATM records, read our medical records, or translate our international communications."

You would think such "alarmist" rhetoric is coming from groups such as the American Civil Liberties Union, the Electronic Privacy Information Center, or the Southeastern Legal Foundation -- all of whom have been critical of TIA.

You would be wrong.

January 2, 2003

Daily Commentary

Interventionism, Allegedly a Middle-of-the-Road Policy

by Ludwig von Mises

[Archives]

Daily Digest

- South Korea and China Act Diplomatically with North Korea
- D.C. Cuts Literacy Program
- New Study Says Global Warming is Forcing Many Species to Migrate

[Archives]

Pocket Constitution
Email Updates
Cato Audio
Cato Store
Cato on Your PDA
Cato University
El Cato

Those words were written in October 1997 by then-Senator John Ashcroft. He was taking issue with the Clinton administration's views on the Internet and proposed regulations and controls. Curiously, today, Attorney General Ashcroft has been deafeningly silent on the issue of TIA. Apparently, what's not good for the goose is okay for the gander.

But Ashcroft's concerns about the future of the Internet then are as valid when it comes to TIA now. Americans should not blindly give in to fear and a sense of vulnerability by giving the federal government (in particular, the executive branch) ever-expansive powers all in the name of homeland security and fighting the war on terrorism. The fundamental question is not whether TIA is a good idea right now because we must cope with a new terrorist threat. The question is whether TIA is a good idea, period -- whether in this, the previous, or successive administrations.

Concerns about TIA are threefold.

First and foremost is the issue of civil liberties. If government had a pristine record and this was the first and only proposal that potentially threatens civil liberties, perhaps the cause for concern might be less. But TIA is being proposed by an administration with a penchant for secrecy and a "trust us, we know what we're doing" attitude. This same administration also gave us the USA PATRIOT Act, which gives the executive branch extraordinary power absent judicial checks and balances. And even though it was explicitly prohibited in the Homeland Security Act, the administration had previously proposed the TIPS (Terrorist Information and Prevention System), which would have made us a nation of snitches.

Second, how might TIA affect the information economy and electronic commerce? TIA is built on the premise of having access to transactional and record-keeping data. But people need to know that private information handed over to Internet service providers, banks, airlines, hotels, and other businesses will not routinely be given to the government and stored in a centralized database that -- despite cybersecurity -- could be hacked.

Third, how effective would TIA be in identifying and catching terrorists? TIA assumes that terrorists act according to certain patterns. If terrorist activity is static and unchanging, then the past could be predictive of the future. But the nature of terrorists is that they morph and adapt -- so they will likely learn the cues and patterns TIA is looking for and then avoid them. And this would increase the likelihood that TIA will mistakenly identify ordinary people as terrorists.

One final caution about TIA: It's being touted as a solution

to "connecting the dots" of intelligence data that weren't connected prior to Sept. 11. But another major intelligence shortcoming was over-reliance on technology and not enough human intelligence. The U.S. government needs to be careful about going back to the future with TIA and falling into the same trap.

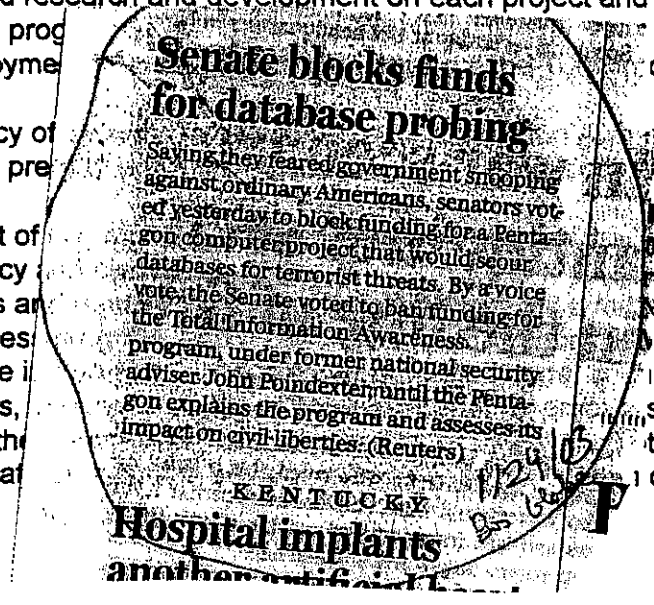
Send this page to a friend

Printer Friendly Version

1000 Massachusetts Avenue, N.W. Washington D.C. 20001-5403
Phone (202) 842-0200 Fax (202) 842-3490
All Rights Reserved © 2002 Cato Institute

From cdt.org:
Senate Votes to Block TIA Pending More Info - The US Senate approved on a voice vote an amendment blocking use of the Defense Department's Total Information Awareness program unless Congress specifically authorizes it after the Administration submits a report the amendment requires about the program and its effect on privacy. The amendment by Sen. Ron Wyden (D-OR) was added to the omnibus continuing appropriations act, the massive spending bill for fiscal 2003, now under consideration in the Senate. Jan. 23, 2003

Wyden Amendment
On 01/17/03, Sen. WYDEN (for himself, Mrs. FEINSTEIN, Mr. REID, Mrs. BOXER, Mr. CORZINE, and Mr. LEAHY) submitted Amendment 59 (SA 59) intended to be proposed by him to the joint resolution H.J. Res. 2, making further continuing appropriations for the fiscal year 2003, as follows:
At the end of title I of division M, add the following:
SEC. 111. (a) **LIMITATION ON USE OF FUNDS FOR RESEARCH AND DEVELOPMENT ON TOTAL INFORMATION AWARENESS PROGRAM.**–Notwithstanding any other provision of law, commencing 60 days after the date of the enactment of this Act, no funds appropriated or otherwise made available to the Department of Defense, whether to an element of the Defense Advanced Research Projects Agency or any other element, or to any other department, agency, or element of the Federal Government, may be obligated or expended on research and development on the Total Information Awareness program unless--
(1) the report described in subsection (b) is submitted to Congress not later than 60 days after the date of the enactment of this Act; or
(2) the President certifies to Congress in writing, that--
(A) the submittal of the report to Congress within 60 days after the date of the enactment of this Act is not practicable; and
(B) the cessation of research and development on the Total Information Awareness program would endanger the national security of the United States.
(b) **REPORT.**–The report described in this subsection is a report, in writing, of the Secretary of Defense, the Attorney General, and the Director of Central Intelligence, acting jointly, that–
(1) contains–
(A) a detailed explanation of the actual and intended use of funds for each project and activity of the Total Information Awareness program, including an expenditure plan for the use of such funds;
(B) the schedule for proposed research and development on each project and activity of the Total Information Awareness prog
(C) target dates for the deployme ormation Awareness program;
(2) assesses the likely efficacy of eness program in providing practically valuable pre r capabilities of terrorists or terrorist groups;
(3) assesses the likely impact of otal Information Awareness program on privacy
(4) sets forth a list of the laws ar e collected by the Total Information Awarenes ns of such laws that will be required to use the i program;
(5) includes recommendations, s, procedures, regulations, or legislation on th tal Information Awareness program to elimina on privacy and


Senate blocks funds for database probing

Saying they feared government snooping against ordinary Americans, senators voted yesterday to block funding for a Pentagon computer project that would scour databases for terrorist threats. By a voice vote, the Senate voted to ban funding for the Total Information Awareness program, under former national security adviser John Poindexter, until the Pentagon explains the program and assesses its impact on civil liberties. (Reuters)

KENTUCKY

Hospital implants

FindLaw | Legal Professionals | Students | Business | Public | News

E-mail@Justice.com | MY FindLaw

FindLaw's Writ
LEGAL COMMENTARY

Looking for a Lawyer?
City or Zip | State | Practice Area
POWERED BY WEST LEGAL DIRECTORY

Legal News | Entertainment | Sports | Newsletters | Supreme Court

Find A Lawyer | Law Jobs | CLE

Lawyer Search | City or ZIP | State | Select a Practice Area | Find

Writ: Commentary

Front Page

Forums
Enron
Tribunals
Terrorism
2000 Elections

Archives
Columnists
Guest Columnists

Law Students

Book Reviews

Message Boards

Legal News
US Law
Supreme Court
Politics
Civil Rights
Crime
Tort
Business
Labor
Tech & IP
Environment

Investigations

International

Entertainment

Sports

News Wires

Legal Documents

FindLaw Features



Print This | Email This

Patriot II:

The Sequel Why It's Even Scarier than the First Patriot Act

By ANITA RAMASASTRY

Monday, Feb. 17, 2003

Soon after the terrorist acts of September 11, Congress passed the USA Patriot Act, which conferred broad new powers upon the federal government. Now John Ashcroft and his scribes at the Justice Department have been working secretly to create new, 120-page draft legislation that, if enacted, would expand greatly upon these already sweeping powers.

This daring sequel to the USA Patriot Act is known internally as the Domestic Security Enhancement Act. It is also nicknamed Patriot II (the name by which I'll refer to it here), or Son of Patriot. On February 7 of this year, a January 9 draft of Patriot II was revealed to the public - but not by the government. It was made public only through a leak.

Even Congress itself, strikingly, appears to have played little or no part in Patriot II's drafting (though it seems that Speaker of the House Hastert was, at least, given the opportunity to review the draft last month, as was Vice President Cheney.).

Perhaps the Bush Administration is looking to repeat its experience with the original USA Patriot Act. Amidst the emotional turmoil after September 11, the Administration introduced the Act and got it enacted in a matter of weeks. The Senate Judiciary Committee had only a brief, one-and-a-half-hour hearing on the Act, in which Attorney General Ashcroft testified but took no questions. In the House, meanwhile, there was no testimony from opponents of the bill.

After September 11, there was at least some rationale for this expedited consideration. Now, however, there is far less exigency. If the introduction of Patriot II in Congress coincides with the Iraq war, it may well be because the Administration has planned it that way, to take advantage of circumstances to ram the bill through both Houses quickly.

Even if Patriot II does end up being introduced in wartime, citizens and their representatives should fight this legislation tooth and nail, for it threatens to take even more of our liberties away. It is a wholesale assault on privacy, free speech, and freedom of

Coming W

Columnis
C. Dorf O
Supreme
Rejects
Racketee
Liability
Abortion

AND: Co
Anita Ra
On Chall
FBI's Spy

Book Revi

Michal B
The Vietn
Trial

- by Joan

Columnist

Akhil Am

Vikram A

Bart Aro

Sherry C

John Dea

Michael

Joanna G

Marci Ha

Julie Hild

Edward

Joanne M

Anita Ra

Supreme Court Center
Election 2000 Center
Recent Case Law
Cases & Codes
FindLaw Library
Legal Dictionary
MY FindLaw

information.

Making Total Information Awareness the Law

Admiral Poindexter's proposed Total Information Awareness (TIA) program, which sought to build data profiles of all Americans, sparked a wide public outcry. Congress recently warned against using TIA as a tool against US citizens. Nevertheless, Patriot II, as draft by the Attorney General and his staff, would begin to make TIA the law.

For instance, under Patriot II, federal agents would not need a subpoena or obtain a court order to access our consumer credit reports. This provision would open the wedge for TIA to be implemented through a huge database. Our credit reports are repositories of a great deal of sensitive information - from our employment history to where we shop, borrow and transact.

To see the information, the feds would only have to certify that they will use the information "in connection with their duties to enforce federal law." Note that they would not have to certify that the person whose information was accessed was suspected of terrorism, or indeed, any other crime. And no one would be notified that their records had been accessed. When a commercial entity requests a consumer's credit report, a note is made in the consumer's file alerting him to this fact.

A Mandate to Collect Genetic Information

Meanwhile, not only data, but genetic information would also be collected by the government if Patriot II were passed.

DNA would be put into a "Terrorist Identification Database." It would contain information not only for proven terrorists, but also "suspected terrorists." And that term would include anyone who was associated with, or had provided money or other support for, groups designated "terrorist."

It might also include protesters, or anyone else the government dislikes. Remember, the original USA Patriot Act defined the new crime of "domestic terrorism" broadly, to encompass "any action that endangers human life that is a violation of any Federal or State law."

Certainly one could envision a disruptive war protester who resisted arrest being tagged as a "suspected domestic terrorist," and forced to provide DNA. Would the government need to get a court order to procure the DNA? Not under Patriot II.

And what if the protester wouldn't comply? That would be a Class A misdemeanor, punishable by up to one year in prison and a $100,000 fine. Anyway, the protester's refusing to give up DNA might be futile - if any other government agency happens to have a blood sample, Patriot II gives the government the right to put it in the new database.

Incredibly, DNA would also be collected from anyone who is, or has been, on probation for any crime, no matter how minor. State governments would be required to collect DNA samples from state probationers and provide them to the federal government.

Anthony

Guest Co

Featured

Unmaskin Throat



A W de w ev identity of h elusive new by John D

Writ Forum

Message

Increasing Surveillance Powers

Database surveillance, under Patriot II, would also be combined with increased active surveillance of citizens.

To assess the change, it's important to remember that the Patriot Act itself already greatly expanded surveillance powers. Now Patriot II would, if enacted, makes it even easier for the government to engage in surveillance of U.S. citizens, without having to establish traditional probable cause under the Fourth Amendment. It would do so by making it easier for law enforcement to avail itself of the Foreign Intelligence Surveillance Court, which issues warrants more easily than federal district courts will.

The FISA Court is meant to address international terrorism, involving mostly noncitizens. Patriot II, however collapses the distinction between domestic and international terrorism, treating wholly domestic criminal acts as subject to the same, looser legal rules that apply to foreign intelligence gathering.

Remember, domestic terrorism is defined very broadly as "any action that endangers human life that is a violation of any Federal or State law." That means anything from getting into a raucous bar fight, to driving recklessly over the state speed limit, could theoretically count. And if the government finds a particular person suspicious, they could cite law violations as far from terrorism as these as a valid excuse for surveillance.

Worse, even those persons who cannot be deemed "domestic terrorists" because they have not broken any law, can alternatively be deemed "foreign powers" under Patriot II - even if they are American citizens or permanent residents. This allows the FBI to get pen registers on American citizens for a foreign intelligence investigation - without having to show any criminal or terrorist connection.

Gagging American Citizens and Cutting Off Their Rights to Sue

If you don't like the government's policies, including these, Patriot II says: Too bad. Don't try to make a federal case out of it - we'll bar you at the courthouse door.

What if you're lucky enough discover that you've been illegally spied on, in violation of your Fourth Amendment rights? Too bad. Patriot II would provide immunity from liability to law enforcement engaging in spying operations against the American people. The proposed act provides a defense for federal agents who engage unauthorized searches and surveillances relating to foreign intelligence when they are acting "pursuant to a lawful authorization from the President or the Attorney General."

What if a disgruntled business competitor chooses to falsely claim to the government that you're a "suspected terrorist"? Again, too bad. Don't consider suing the competitor, no matter what consequences ensure Patriot II eliminates civil liability for businesses and employees that report "suspected terrorists" to the federal government, no matter how malicious or unfounded the tip may be.

Like TIA, Operation TIPS - which would have enlisted government employees to spy on citizens - elicited public outcry. But this is TIPS

all over again. If they like, your package courier or cable guy can report you to the feds with impunity.

Broadly Criminalizing Encryption of Evidence

Meanwhile, in your search for a shred of privacy that might remain to you, don't even think about trying to protect your email. Under Patriot II, the government may go after you for that, too.

Specifically, Patriot II, as currently drafted, would makes it a new, separate crime to use encryption in the commission of another crime. To be convicted, the defendant must be shown to have "knowingly and willfully use[d] encryption technology to conceal any incriminating communication" relating to a federal felony he is committing, or attempting to commit.

The "federal crime" limitation may seem significant, until you realize that "domestic terrorism" - which can be based on a state law violation - is a federal crime. Remember, too, how loosely "domestic terrorism" is defined, in a way that could encompass a protester's resisting arrest, and if you do, you may reasonably fear using encryption even if you are not engaged in any criminal activity at all.

What if your encrypted email about protest planning is deemed "incriminating evidence" of your plan to resist arrest at the protest? You could be looking at five to ten.

The penalty for this offense alone would be up to ten years in prison. In addition, a Justice Department analysis included with the proposal suggests that the illegal encrypting ought to carry a mandatory minimum term of five years in prison.

Notably, the federal felony relating to the "incriminating communication" need not be an act of terrorism. It could be any federal crime, from the most major to the most minor, the most violent to the most excruciatingly technical. And that's frightening.

For instance, if a peer-to-peer website's users swap files, thus violating the Digital Millenium Copyright Act, and encrypt the files they are swapping, they may automatically face five years in prison, and could serve ten, for the encryption alone.

What is most shocking about the new encryption crime is that it is not limited to terrorism. This is the first attempt to regulate encryption domestically at all.

Shrouding Government Actions in Secrecy

While the government, according to Patriot II, has the right to know virtually everything about you, you have little right to know anything about the government.

Current grand jury secrecy rules apply only to jurors, prosecutors and courtroom staff. Patriot II would expand them to apply to witnesses too - meaning that ordinary citizens could not discuss their testimony with anyone but their attorney. In theory, they'd have to keep mum even with spouses or children, or face serious consequences.

What if they've been improperly subpoenaed in the first place? Under

Patriot II, too bad: Neither individuals nor organizations may move to try to quash a federal grand jury subpoena.

Will the grand jury itself at least remain independent? Nope. Patriot II allows the federal government to place gag orders on both federal and state grand juries, and to take over the proceedings.

Detentions will be similarly shrouded in an atmosphere of dead secrecy. The Justice Department's position on detainees is that if they are held incommunicado indefinitely without being charged with a crime, they need not be publicly identified. Patriot II would make that dubious position the law.

Meanwhile, if you do happen to somehow find out the identity or whereabouts of - or anything else about - a detainee, it would be criminal under Patriot II to reveal it. And that's the case even if you are the detainee's parent, spouse, or child.

Okay, you might ask, this is a lot of secrecy, but isn't it at least somewhat limited? Can't I at least use the Freedom of Information Act (FOIA) to figure out what the government is doing when it's not secretly detaining people, or secretly conducting grand jury proceedings?

No. Under Patriot II, FOIA would not extend to information "specifically exempted from disclosure by statute." What kind of statutes? Well, the USA Patriot Act might be one. Patriot II might be another.

It's a clever strategy: Collect private information. And then when citizens try to find out what you've collected, cite their own privacy right back at them as a reason not to divulge it.

If it seems farfetched to think the government could invoke privacy in this instance, consider that Ashcroft actually cited detainees' privacy as a reason not to release their names to the press, the public, or even their families.

Denaturalization: The Citizenship Death Penalty

In sum, Patriot II puts in jeopardy the First Amendment right to speak freely, statutory and common law rights to privacy, the right to go to court to challenge government illegality, and the Fourth Amendment right against unreasonable searches and seizures. But that's not all.

It also puts in jeopardy perhaps the most basic right of all: The right to walk the streets in safety without being "disappeared" by the government. Chileans have not always enjoyed this right. Americans, until now, always have.

Suppose you, as a citizen, attended a legal protest for which one of the hosts, unbeknownst to you, is an organization the government has listed as terrorist. Under Patriot II, you may be deported and deemed no longer an American citizen.

Under Patriot II, if you are simply suspected of terrorist activity, this can occur. More specifically, a U.S. citizen may be expatriated "if, with the intent to relinquish his nationality, he becomes a member of, or provides material support to, a group that the United Stated has

designated as a 'terrorist organization'."

How can you tell if the citizen wanted to relinquish citizenship? Under Patriot II, the intent can be inferred from conduct. So any association with even the legal activities of a designated group, plus any act that can be interpreted as disloyal to the United States, can mean you are deported, and no longer considered a citizen.

No Sunset Provisions for Patriot II Mean We Are Stuck with It If It Passes

The original USA Patriot Act has sunset provisions, under which the Act will expire if not renewed in five years. Patriot II, however, does not have such provisions. Indeed, it would go so far as to remove this important check from the original Patriot Act. So if Congress, and the American people don't focus carefully on Patriot II, even in the midst of impending war, we may be stuck with both Patriot Acts indefinitely.

Especially for that reason, Congress and the public need to learn more. Senator Patrick Leahy has argued, for instance, that before the Department of Justice asks Congress for more powers, it needs to disclose how it is using the ones it already has. Instead, the Department has so far repeatedly balked at both FOIA requests from the press and the public and requests from Congress for more detailed reporting pursuant to USA Patriot Act.

At the very least, Congress and the public should insist on a full understanding of what the Justice Department is doing before granting the executive branch still more authority via Patriot II .

What Do You Think? Message Boards

Anita Ramasastry is an Assistant Professor of Law at the University of Washington School of Law in Seattle and the Associate Director of the Shidler Center for Law, Commerce & Technology. Her prior columns on post-September 11 terrorism-related legislation can be found in the archive of her columns on this site.

FindLaw RESOURCES

LEGAL NEWS: Top Headlines · Supreme Court · Commentary · Crime · Cyberspace · International
US FEDERAL LAW: Constitution · Codes · Supreme Court Opinions · Circuit Opinions
US STATE LAW: State Constitutions · State Codes · Case Law
RESEARCH: Dictionary · Forms · LawCrawler · Library · Summaries of Law
LEGAL SUBJECTS: Constitutional · Intellectual Property · Criminal · Labor · more...
GOVERNMENT RESOURCES: US Federal · US State · Directories · more...
INTERNATIONAL RESOURCES: Country Guides · Trade · World Constitutions · more...
COMMUNITY: Message Boards · Newsletters · Greedy Associates Boards
TOOLS: Office · Calendar · Email · FAX · West WorkSpace · FirmSites

Advertising Info · Add URL · Help · Comments Jobs@FindLaw · Site Map

Company | Privacy Policy Disclaimer Copyright © 1994-2003 FindLaw

http//legis.state.nm.us/Sessions/03%20Regular/memorials/house/HJM040.html

46th legislature - STATE OF NEW MEXICO - first session, 2003 INTRODUCED BY Max Coll

A JOINT MEMORIAL

AFFIRMING CIVIL RIGHTS AND LIBERTIES; DECLARING OPPOSITION TO FEDERAL MEASURES THAT INFRINGE ON CIVIL LIBERTIES.

WHEREAS, the state of New Mexico is proud of its long and distinguished tradition of protecting the civil rights and liberties of its residents; and

WHEREAS, New Mexico has a diverse population, including immigrants and students, whose contributions to the community are vital to its economy,
culture and civic character; and

WHEREAS, the preservation of civil rights and liberties is essential to the well-being of a democratic society; and

WHEREAS, federal, state and local governments should protect the public from terrorist attacks such as those that occurred on September 11, 2001 and should do so in a rational and deliberative fashion to ensure that a new security measure will enhance public safety without impairing constitutional rights or infringing on civil liberties; and

WHEREAS, government security measures that undermine fundamental rights do damage to American institutions and values that the residents of New Mexico hold dear; and

WHEREAS, the house of representatives believes that there is no inherent conflict between national security and the preservation of liberty and that Americans can be both safe and free; and

WHEREAS, federal policies adopted since September 11, 2001, including provisions in Public Law 107-56, known as the USA Patriot Act, and related executive orders, regulations and actions threaten fundamental rights and liberties by

A. authorizing the indefinite incarceration of non-citizens based on mere suspicion and the indefinite incarceration of citizens designated by the president as "enemy combatants" without access to counsel or meaningful recourse to the federal courts;

B. limiting the authority of federal courts to curb law enforcement abuse of electronic surveillance in anti-terrorism and ordinary criminal investigations;

C. expanding the authority of federal agents to conduct so-called "sneak and peek" or "black bag" searches, in which the subject of the search warrant has not been notified that his or her property has been searched;

D. granting federal law enforcement and intelligence agencies broad access to personal, medical, financial, library and educational records with little, if any, judicial oversight;

E. chilling constitutionally protected speech through overly broad definitions of "terrorism";

F. driving a wedge between immigrant communities and the police that protect them by encouraging involvement of state and local police in the enforcement of federal immigration law; and

G. permitting the federal bureau of investigation to conduct surveillance of religious services, internet chat rooms, political demonstrations and public meetings of any kind without evidence that a crime has been or may be committed; and

WHEREAS, these new powers pose a particular threat to the civil rights and liberties of the residents of New Mexico state who are or who are assumed to be Arab, Muslim or of South Asian descent; and

WHEREAS, other communities throughout the country have enacted resolutions reaffirming support for civil rights and civil liberties in the face of government policies that threaten these values and have demanded accountability from law enforcement agencies regarding their use of these new powers;

NOW, THEREFORE, BE IT RESOLVED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO that it

A. affirm its strong support for fundamental constitutional rights and its opposition to federal measures that infringe on these rights and liberties;

B. affirm its strong support for the rights of immigrants and oppose measures that single out individuals for legal scrutiny or enforcement activity based on their country of origin;

C. direct the New Mexico state police to

(1) refrain from participating in the enforcement of federal immigration laws;

(2) seek adequate written assurances from federal authorities that residents of the state of New Mexico and individuals in the custody of the state who are placed in federal custody will not be subjected to military or secret detention or secret immigration proceedings without access to counsel and, absent such written assurances, refrain from assisting federal authorities to obtain custody of these individuals;

(3) refrain from engaging in the surveillance of individuals or groups of individuals based on their participation in activities protected by the First Amendment to the United States constitution, such as political advocacy or the practice of a religion, without reasonable and particularized suspicion of criminal conduct unrelated to the activity protected by the First Amendment to the United States constitution;

(4) refrain from using race, religion, ethnicity or national origin as a factor in selecting who is subject to investigatory activities unless race, religion, ethnicity or national origin is part of the description of a specific suspect to be apprehended;

(5) refrain, whether acting alone or with federal law enforcement officers, from collecting or maintaining information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activity and there are reasonable grounds to believe that the subject of the information is or may be involved in criminal conduct;

(6) provide advance or simultaneous notice of the execution of a search warrant to any resident of the state of New Mexico whose property is the subject of the search and refrain from participating in a joint search with any law enforcement agency absent assurances that such a notice will be provided;

(7) refrain from undertaking or participating in any initiative, such as the terrorist information and prevention system, also known as TIPS, that encourages members of the general public to spy on their neighbors, colleagues or customers;

(8) refrain from the practice of stopping drivers or pedestrians for the purpose of scrutinizing their identification documents without reasonable and particularized suspicion of criminal activity; and

(9) report to the legislature and the interim corrections oversight and justice committee, any request by federal authorities that, if granted, would cause agencies of the state to exercise powers or cooperate in the exercise of powers in apparent violation of a city ordinance or the laws or constitution of this state or of the United States;

D. direct public schools and institutions of higher education to provide notice to individuals whose education records have been obtained by law enforcement agents pursuant to Section 507 of the USA Patriot Act;

E. direct public libraries to post in a prominent place within the library a notice as follows "WARNING

Under Section 215 of the federal USA Patriot Act (Public Law 107-56), records of books and other materials you borrow from this library may be obtained by federal agents. This law also prohibits librarians from informing you if records about you have been obtained by federal agents. Questions about this policy should be directed to Attorney General John Ashcroft, Department of Justice, Washington, DC 20530."; and

F. direct the state official in charge of homeland security for New Mexico to seek periodically from federal authorities the following information in a form that facilitates an assessment of the effect of federal anti-terrorism efforts on the residents of the state of New Mexico and provide to the legislature and the interim corrections oversight and justice committee, no less than once every six months, a summary of the information obtained

(1) the names of all residents of New Mexico who have been arrested or otherwise detained by federal authorities as a result of terrorism investigations since September 11, 2001, and

(a) the location of each detainee;

(b) the circumstances that led to each detention;

(c) the charges, if any, lodged against each detainee; and

(d) the name of counsel, if any, representing each detainee;

(2) the number of search warrants that have been executed in New Mexico without notice to the subject of the warrant pursuant to Section 213 of the USA Patriot Act;

(3) the extent of electronic surveillance carried out in the state pursuant to powers granted in the USA Patriot Act;

(4) the extent to which federal authorities are monitoring political meetings, religious gatherings or other activities within New Mexico that are protected by the first Amendment of the United States constitution;

(5) the number of times education records have been obtained from public schools and institutions of higher learning in New Mexico pursuant to Section 507 of the USA Patriot Act;

(6) the number of times library records have been obtained from libraries in New Mexico pursuant to Section 215 of the USA Patriot Act; and

(7) the number of times records of books purchased by store patrons have been obtained from bookstores in New Mexico pursuant to Section 215 of the USA Patriot Act; and

BE IT FURTHER RESOLVED that copies of this memorial be transmitted to Senators Jeff Bingaman and Pete Domenici and Representatives Tom Udall, Heather Wilson and Steve Pearce, with a letter urging them to monitor federal anti-terrorism tactics and to work to repeal provisions of the USA Patriot Act and other laws and regulations that infringe on civil rights and liberties; and

BE IT FURTHER RESOLVED that copies of this memorial be transmitted to President George W. Bush and Attorney General John Ashcroft; and

BE IT FURTHER RESOLVED that a copy of this memorial be transmitted to the state official in charge of homeland security for New Mexico; and

BE IT FURTHER RESOLVED that copies of this memorial be transmitted to the New Mexico state police and to all public schools, institutions of higher education and public libraries within the state of New Mexico.

Brown, L. Gail

From: Brown, L. Gail
Sent: Thursday, April 17, 2003 8:44 AM
To: Daniels, Ann; Duncan, Susan; Cayes, Carlene; Morin, Donna; Williams, Chris; Fitz, Margaret; Babson, David; Tholl, John; Almy, Susan; Kurk, Neal; Smith, Marjorie; Smith, Marjorie; Buhlman, David; Spiess, Paul; Dokmo, Cynthia; Hess, Dave; Bergin, Peter; Welch, David; Welch, David
Subject: Senate Interstate Cooperation

Please see attached revised notice for April 23, 2003. At the request of Rep. Almy we have deleted HCR 9 and will schedule at a later date.



April 23 notice #2.doc

Brown, L. Gail

From: Susan Almy [Susan.Almy@valley.net]
Sent: Wednesday, April 16, 2003 5:10 PM
To: Brown, L. Gail
Subject: HCR9

Could you please ask Sen Gatsas if he would be willing and able to reschedule this to a different day, as I have to be in Lebanon before 4PM that day for a vital function I am in charge of? I am the prime on HCR9. There is a large group of reps working on this (we will probably take more than 15 minutes but maybe can condense down) so if he can't, they can probably get enough of them there to handle it without me.

At 11:45 AM 4/16/03 -0400, you wrote:

Committee Report

STATE OF NEW HAMPSHIRE

SENATE

REPORT OF THE COMMITTEE

Date:

THE COMMITTEE ON Interstate Cooperation

to which was referred House Concurrent Resolution 9

AN ACT urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

VOTE: 2-0

Having considered the same, report the same without amendment and recommend that the bill: **OUGHT TO PASS.**

Senator Robert Clegg, Jr.
For the Committee

HCR9 Docket

Next|Prev|Results List|Main|Bill Status

Bill Title: urging the President and the Joint Chiefs of Staff to abandon the Total Information Awareness Initiative.

Date	Body	Description
1/9/2003	H	Introduced and ref to St-Fed Rel & Vets Affs; HJ 12, p191
1/21/2003	H	Copy to Chairman on 1/21/2003
1/22/2003	H	Hearing Feb 4 11:00 RM306,LOB
3/6/2003	H	Maj Report OTP for Mar 12 (Vote 14-1;CC)
3/12/2003	H	Adopted; HJ23, p552 + 591
3/13/2003	S	Introduced and Ref. to Interstate Cooperation; SJ 8, Pg.108
5/1/2003	S	Hearing; May 7, 2003, Room 101, LOB, 3:15 p.m.; SC21
5/29/2003	S	Committee Report; Ought to Pass, [06/05/03]; SC25
6/5/2003	S	Ought to Pass; SJ 19, Pg.629
6/5/2003	S	Sen. Clegg Moved Laid On Table, MA, VV; SJ 19, Pg.629

Next|Prev|Results List|Main|Bill Status

Docket Abbreviations