

Free Congress Foundation letter to Members of Congress, Oct. 2, 2001

October 2, 2001

Dear Member of Congress:

While we commend the Administration for responding quickly and initiating the process for reform of our terrorism policy in response to the tragedies of September 11th, we also laud the Congress for taking the time to consider the implications of these proposals. We reaffirm the importance of a vigorous anti-terrorist posture by the federal government and the most severe penalties possible for those guilty of such unspeakable atrocities. This is not the time for knee-jerk appeals to civil liberties -- but neither is it the time to rush headlong into an expansion of the surveillance state and abridge the Constitutionally-protected rights of US citizens. With regards to anti-terrorist proposals now circulating through the Congress, it is important that a deliberate course be followed before granting the Executive wide discretionary powers, and that measures having little or nothing to do with fighting terrorism not be passed in a fervor of fear or revenge.

To that end, we make the following recommendations. Certain sections of the Administration's proposal go beyond what Congress should consider and must be rejected. They include:

- * Section 105 (Use of wiretap information from foreign governments),
- * Section 156 (Business records),
- * Section 158 (Disclosure of educational records),
- * Section 352 (Notice),
- * Section 406 (Restraint of property subject to forfeiture), and
- * Section 505 (Assistance to countries co-operating against international terrorism).

There are also reports that the Treasury Department may propose further additions to the bill within its broad areas of financial crime, firearms, explosives (including gunpowder) and arson. This late in the process, even the strongest supporters of the bill would rightly be very reluctant to add further complex, controversial and divisive issues such as these. Any provisions that have not already been discussed with the respective Judiciary committees and all interested parties should be reserved for further discussion at a later date, if they are to be considered at all.

- * Attempts to graft the global "Know Your Customer" proposals, such as S398 and S1371, to an anti-terrorism measure should be rejected out of hand. These proposals would not have prevented the recent tragedies nor given us more security but would violate our financial privacy and subject us to "profiling" for "suspicious" behavior; they would undermine public confidence in financial institutions and add to regulatory burden at a time when the economy is in a precarious state. The proposals would undo our proper checks and balances by giving power to the secretary of the Treasury sole discretion to prohibit certain types of financial transactions, all international financial transactions with certain institutions, and ultimately prohibit all international financial

transactions with other countries. This approach of the Financial Action Task Force has caused economic dislocations for many small developing economies, especially in the Caribbean (which potentially undermines our national security), without any appreciable benefit against the war on terrorism. The proposal to criminalize the use of cash ("bulk cash smuggling") in certain cases amounts to capital controls, could cause serious economic problems and would be subject to abuse which the Supreme Court and Congress have already had to address (in the Civil Asset Forfeiture Act of 2000).

These other sections of the proposal should be modified:

* Section 101 (Modification of Authorities relating to use of pen registers and trap and trace devices): This provision extends the use of pen register and trap and trace orders to the Internet. It also allows a Federal Judge having jurisdiction over the issuance of such an order to issue one that is valid anywhere within the United States. Congress should consider expressly stating that the information to be obtained is not to include the content of the communication. Header information is acceptable but not the subject line. Additionally, a challenge to an order should be permitted in the jurisdiction it was issued or where the order was served.

* Section 103 (Authorized disclosure): The definition of "investigative and law enforcement officer" should be narrowed to only include President, Vice President, national security and intelligence personnel, and law enforcement officials in connection with performing official duties.

* Section 106 (Interception of computer trespassers communications): Turns Internet Service Provider (ISP) "terms of service" into license to intercept email without court order. The Administration proposal says that anyone accessing a computer "without authorization" has no privacy rights and can be tapped by the government without a court order, if the operator of the computer system says its okay. This means that if an ISP's terms of service say "no downloading copyrighted music," anytime the ISP finds that someone is downloading music, the ISP can authorize the government to tap all of that person's communications. A better approach would be to allow ISPs to seek government assistance when their systems have been commandeered by a hacker.

* Section 108 (Nationwide service of search warrants for electronic evidence): This provision would allow the FBI to go to any judge in the country with arguable jurisdiction over an investigation for a massive search warrant reaching electronic communications -- potentially of large numbers of people, located all over the country. These expansive powers are not limited to terrorism offenses, but, rather, are applicable to any person or organization which has become an investigatory target. Advocates of this section argue that, by limiting an electronic search warrant to a "court with jurisdiction over the offense under investigation," they have somehow limited its potential for abuse. Unfortunately, by alleging a "conspiracy," for example, the government could argue that the offense took place at the residence or business of any member of the organization. The Second Amendment community, among others, has been victimized by this type of forum shopping, as anti-gun activists have sought out the

judges most antithetical to our beliefs. We will fight hard to prevent changes which expand this potential for abuse.

* Section 151 (Period of orders for electronic surveillance of non-United States persons under foreign intelligence surveillance): Allows initial tap of home phone and secret searches of home (black bag jobs) to run for one year without judicial review. Applies only to aliens in the US. Already, foreign intelligence taps of office phones and secret searches of offices can run for one year, while intelligence taps on home phones run for 90 days, three times as long as criminal wiretaps, and secret searches can be carried out repeatedly for 45 days. The Administration proposal would extend these periods to one year. Even for foreign nationals, this is too long to go without the judge having to review the case. At the least, the government should have to come back within 90 days and 45 days after the first authorization to show that the search was bearing fruit and that the suspicions about the target were being borne out.

* Section 152 (Multi-point authority): This section would allow the government to compel a common carrier, landlord, custodian or other person not specified in a court order to provide information and assistance with electronic surveillance if a "court finds that the actions of the target of the application may have the effect of thwarting the identification of a specific person." In the words of DoJ, "...the FBI could simply present the newly discovered carrier, landlord, custodian, or other person with a generic order issued by a Court, and could then effect FISA coverage as soon as technically feasible." Thus, as a suspect moves from place to place, the government can expand its demands to every person or organization the suspect comes in contact with, without the nicety of judicial review or consent. If, for instance, a suspect is a delivery man for a common carrier, a client of that common carrier might well become a subject of a government wiretap, even though it is not suspected of any crime. Conservatives and civil libertarians fought a heated battle over a similar effort in the 1996 terrorism bill. The section has become no less offensive over time.

* Section 153 (Foreign intelligence Information): Allows the government to initiate wiretaps in criminal investigations under the weaker standards permitted for foreign intelligence taps, thereby circumventing the relatively stricter provisions of the wiretap law. Applies to US citizens as well as aliens, and not limited to terrorism cases. Foreign intelligence wiretaps, which were not supposed to be used for the purpose of gathering evidence in criminal cases, lack many of the protections afforded under the regular wiretap law - they can be initiated without suspicion of criminal conduct, they can collect a wider range of information for a longer period of time, there is usually never notice to the target of the surveillance, even after the investigation ends, and when they are used as evidence in a criminal trial, the predicate for the tap cannot be challenged by the defendant. The real issue is to ensure consultation between intelligence agents and criminal investigators - that would not threaten the foundation of FISA. Therefore, rather than the change proposed by the Administration, a much better approach would be to amend FISA to expressly state that consultation between the foreign intelligence/counterintelligence agents and criminal prosecutors does not deprive an intelligence tap of its primary purpose.

* Section 154 (Foreign intelligence information sharing): This section would allow grand jury and electronic information, obtained during a criminal investigation, to be shared freely with "ANY federal law enforcement-, intelligence-, protective-, or national-defense personnel, or [with] any federal personnel responsible for administering the immigration laws of the United States." This list of "intelligence-sharers," arguably encompassing millions of federal employees, does not require that the recipient be conducting any investigation to which this highly privileged information would be relevant. At the very least, this provision should be amended to add the following language: "if and only if the personnel receiving the information are conducting an active investigation which is relevant to the information."

* Section 155 (Pen register and trap and trace authority): Pen registers and trap and trace authority in regard to FISA was changed in 1998. Currently, the target must be or had engaged in international terrorism that may violate U.S. criminal law or must be an agent of a foreign power. Because this section lowers the standard for a FISA pen register and trap and trace, it should not apply to U.S. citizens.

* Section 157 (Miscellaneous national-security authorities): Consumer Credit Protection standards are lowered by this section. Currently, the target must be a foreign power, a person who is not a United States person, and an official of a foreign power; or an agent of a foreign power who has or is engaging in international terrorism that may violate U.S. criminal law. The language in the statute (15 U.S.C 1681(u)) should be maintained. Alternatively, any changes aiming to lower the standard for access to consumer credit records, in the name of counterintelligence, should not apply to U.S. citizens.

* Section 201 (Definitions relating to terrorism): Congress should be careful not to tar with the terrorist label innocent spouses or children of suspects, nor those who may have unknowingly given funds to an organization that supports terrorism. Also, giving funds solely for humanitarian purposes should not be a deportable offense.

* Section 202 (Mandatory detention of suspected terrorists): Expansion of the Attorney General's power to detain immigrants suspected of terrorism should be done carefully and with an eye to due process.

* Section 305 (Biological weapons): Needs to be more narrowly tailored such as dropping the list of biological agents compiled by HHS.

* Section 309 (Definition): This provision defines the term " Federal terrorism offense". Other provisions of the bill provide for prosecution without time limitation and increased penalties for those involved in illegal conduct that meets this definition. The proposal defines the term " Federal terrorism offense" as "the violation of, or an attempt or conspiracy to violate "and then lists approximately 27 existing crimes. The most troublesome aspect of this definition is that it includes crimes that common sense tells us are not terrorist acts in the sense that those acts are generally understood. Some of the

offenses listed relate too: injury to buildings or property over and under \$1,000, violence against maritime navigation, conspiracy to injure property of a foreign government, arson, assault on a member of congress and protection of computers. The prospect of prosecutors bringing terrorism charges against some one who defaces a government building, assaults a congressman or engages in computer hacking should, at the very least, call this provision into question.

Congress should consider either limiting the offenses that constitute the definition of 'federal terrorism offense ' to only those crimes which common sense dictates is a terrorist act or if all the crimes are to remain include a terrorist mens rea as an element of the crime. Unfortunately, the inclusion of Section 351, Title 18, in the list of terrorism predicates might make PETA a terrorist organization because one of its members hit the Secretary of Agriculture with a pie.

Several suggestions have been made for improving this language: One would incorporate the "intent test" contained in the definition of "international terrorism" in section 2331 of Title 18. Another would require a showing of over \$10,000 in intended damages or an intent to cause death or serious bodily injury. Whatever alternative is chosen, the current definition is anathema to virtually every conservative organization.

Section 354 (Grand jury matters): Grand Jury information is currently protected. This section aims to permit the information to be shared with a broad range of U.S. officials. The list should be shortened to U.S. law enforcement and intelligence personnel. Furthermore, it should only apply to terrorism cases and court approval should be required before the release of any grand jury information.

Section 403 (Assets of terrorist organizations): This section is overly broad and should have the same limits as we identified in our recommendation for changes to Section 309.

Section 405 (Disclosure of tax information in terrorism and national-security investigations): This section needs to be tightened so that the requested records are relevant to the investigation being conducted by the requesting party.

Section 408 (Extraterritorial Jurisdiction): This section should be narrowed to apply to terrorism cases specifically.

Necessary adjustments to the law in the fight against terrorism are applauded by all. But expanding of the police state and curtailing the Constitutional rights of Americans just hands the eats away at who and what we are. Tearing down America and her Constitution would only give the anti-Americans another victory in addition to the carnage they have already wreaked. Please don't give the terrorists that victory. Think before you vote.

If you have any questions, please contact J. Bradley Jansen, deputy director of the Center for Technology Policy at Free Congress Foundation by e-mailing him at bjansen@freecongress.org or by calling (202) 204-5324.

Signed,

Paul M. Weyrich
President, Free Congress Foundation