AMERICAN CIVIL LIBERTIES UNION

WASHINGTON LEGISLATIVE OFFICE
Laura W. Murphy
Director

1333 H Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

To: Interested Persons

From: Timothy H. Edgar, ACLU legislative counsel

Re: DOJ letter opposing SAFE Act

Date: February 6, 2003

The Attorney General's letter recommending a veto of the Security And Freedom Enhanced (SAFE) Act of 2003 is based on hyperbole and slanted legal analysis, not facts. Congress should still enact SAFE this year.

The bipartisan SAFE Act is a measured, informed response that adds safeguards to key provisions of the USA PATRIOT Act that threaten fundamental American civil liberties. To set the record straight, *the SAFE Act does not repeal any provision of the USA PATRIOT Act, much less take away any of the government's pre-9/11 anti-terror powers*.

Notably absent from the Attorney General's letter is any real-life terrorism case (or indeed any case) where the prudent limits of the SAFE Act on USA PATRIOT Act surveillance powers would actually have impeded an investigation. Instead, the letter mischaracterizes the provisions of the SAFE Act in an effort to frighten potential co-sponsors of the legislation.

Surveillance powers amended by the SAFE Act including roving wiretaps in intelligence investigations, searches of library and other personal records, and "sneak and peek" warrants. The SAFE Act preserves all these surveillance powers while amending them to restore meaningful judicial and Congressional oversight.

Roving wiretaps. Prior to the passage of the USA PATRIOT Act, the government could obtain an electronic surveillance order of a suspected international terrorist either by obtaining a criminal wiretap order based on probable cause of criminal activity,[1] or by obtaining an intelligence wiretap order under the Foreign Intelligence Surveillance Act (FISA).

[1] Criminal wiretaps are also called "Title III wiretaps" because they were authorized by Title III of Pub. L. No. 90-351, the Omnibus Crime Control and Safe Streets Act of 1968, now codified at chapter 119 of Title 18, United States Code.

"Roving wiretaps," which permit the government to conduct surveillance without obtaining a new court order when the suspect changes from one facility (usually a telephone) to another, *were available for suspected terrorists* in criminal terrorism investigations. To obtain a roving wiretap in a criminal investigation, the government has to specify a target and the person conducting the surveillance has to "ascertain" that the target is using the facility.[2]

Section 209 of the USA PATRIOT Act made roving wiretaps available in intelligence (FISA) investigations. However, the ascertainment requirement – which ensures the target is actually using the telephone the government is tapping – was not included. As a result, the government could easily listen into conversations of entirely innocent people simply because it supposed, wrongly, that a target might be using that telephone. The danger of intercepting innocent conversations is compounded in intelligence investigations, which are not limited to targets who are necessarily suspected of any criminal activity.

Section 314(a)(2) of the Intelligence Authorization Act for FY2002, passed shortly after the USA PATRIOT Act, compounded the problem by creating what was, until then, an entirely unknown surveillance power – the "John Doe" roving wiretap. A roving wiretap, in theory, follows a target rather than a particular facility or telephone. However, because of the Intelligence Act's amendment, the government may now, for the first time, obtain a wiretap order without specifying either the telephone *or* the target. As a result, the government can listen into any telephone if it believes an unknown suspect might be using it.

The Attorney General's letter attempts to defend this entirely novel type of wiretap – and escape the "John Doe" roving wiretap moniker – by noting that the order still requires the government to provide a physical description of the unknown suspect. The letter fails to acknowledge the obvious potential for invasion of privacy in a wiretap order that does not apply to a particular telephone, or even a particular person, but lets the government listen in to any telephone the government thinks might be used by a person that happens to meet the physical description of some unknown suspect.

Importantly, the government must specify the "identity" of the target – not necessarily the target's real name. Justice Department officials have long interpreted this requirement of the criminal roving wiretap statute not to require knowledge of the target's true name. For example, a roving wiretap order could be granted if the government knew of a suspect only by an alias.

In sum, the SAFE Act permits roving wiretaps in intelligence investigations, but imposes two safeguards for such wiretaps that are already required for criminal roving wiretaps –

[2] *See* 18 U.S.C. § 2518(11)(b)(ii) (providing that a roving wiretap must "identif[y] the person believed to be committing the offense and whose communications are likely to be intercepted,"); *id.* at (12) (providing that interception pursuant to a roving wiretap "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order.")

that the government specify the target and ascertain the target is actually using the facility.

Wiretaps are the most intrusive form of surveillance known to the law. It is not asking too much to require the government, when it seeks a surveillance order than can jump from telephone to telephone, that it at least specify whom the order is supposed to be following.

Finally, the Attorney General's letter does not even attempt to defend the lack of an ascertainment requirement for FISA roving wiretaps.

"Sneak and peek" warrants. The Attorney General's letter fails to acknowledge that, prior to passage of the USA PATRIOT Act, there was *no statutory authority* for the practice of issuing "sneak and peek" warrants – criminal search warrants where notice of the execution of the warrant was delayed. The Federal Rules of Criminal Procedure – which governs the procedure for issuing search warrants – provided no express exception to the rule requiring service of warrants at the time a search was conducted.

While some courts had approved the practice in limited circumstances, two federal circuit courts of appeals that ruled on sneak and peek warrants prior to 9/11 had done so only pursuant to limitations that were swept away by the USA PATRIOT Act. For example, these courts had imposed a presumptive seven-day time limit for the delay.[3] The Supreme Court had yet to decide whether sneak and peek warrants were authorized by statute or the Constitution (except in the specific context of electronic surveillance which is authorized by statute).[4] In its most recent pronouncement on the subject, the Supreme Court, in an opinion written by Justice Thomas, held that the principle requiring notice for the execution of a warrant (often called the "knock and announce" rule) is not merely a common law principle, but is a constitutional rule based on the Fourth Amendment. *Wilson* v. *Arkansas*, 514 U.S. 927 (1995).

The USA PATRIOT Act differs from prior law in that it does not include any specific time limit, allowing a delay of notice to be extended for any "reasonable" time period. The Act also authorizes such searches not only in specific instances, but whenever the government shows notice would "seriously jeopardize" a prosecution or "unduly delay" a trial.

The SAFE Act merely limits the reasons for "sneak and peek" warrants to three specific circumstances – that notice would cause (1) the life or physical safety of a person (such as a witness) to be put in danger, (2) flight from prosecution, or (3) destruction of evidence. The Attorney General's letter simply mischaracterizes the SAFE Act when it claims it would prohibit a judge from approving a delay if notice would allow a suspect's

[3] See U.S. v. Villegas, 899 F.2d 1324, 1337 (2nd Cir. 1990) (imposing a renewable seven-day notice requirement for "sneak and peek" searches); United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (same).

[4] *See Dalia* v. *United States*, 441 U.S. 238 (1979) (approving a secret search for the purpose of installing bugging equipment).

"associates to go into hiding, flee, change their plans, or even accelerate their plots." Clearly, the SAFE Act standard would permit a delay if the government could show any of the things the Attorney General's letter mentions.

Finally, this letter continues to rely on hypothetical, rather than real-life, examples of a sneak and peek search involving a suspected terrorist. While the Justice Department has reported widespread use of "sneak and peek" search warrants in ordinary criminal cases, the Department still has not provided even one example of how such a warrant has been used in any terrorism case – much less an example of a "sneak and peek" warrant in a terrorism case that could not have been obtained under stricter standards.

The letter also fails to acknowledge that the government can obtain an intelligence search warrant under FISA – which is always secret – for a physical search involving a suspected international terrorist, even where the SAFE Act's standards for criminal "sneak and peek" searches could not be met.

Searches of Library and Other Personal Records.

Prior to passage of the USA PATRIOT Act, FISA records searches were limited to certain (generally travel-related) business records of a suspected foreign agent. Section 215 of the USA PATRIOT Act expanded this power to include any and all "tangible things," including library records, medical records, genetic information, membership lists of organizations, and other sensitive records and eliminated the requirement of individual suspicion.

The SAFE Act preserves the government's new power to obtain any and all records under FISA – including library records – but does put back into place the requirement of individual suspicion that protects the records of innocent people from being obtained by the government.

The Attorney General has publicly revealed – in a speech denouncing the American Library Association – that there have been no FISA records searches at all since September 11, 2001. Astonishingly, the Attorney General's letter still claims that restoring some requirement of individual suspicion for FISA records searches would harm anti-terrorism investigations. If the government is not using a power at all, amending the standards for the use of the power will have no effect on its investigations.

The Attorney General's letter also inappropriately compares the standards for production of records pursuant to a criminal grand jury subpoena with those for production of records under FISA. The government can and does use grand jury subpoenas on a regular basis to obtain records in terrorism investigations. Nothing in the SAFE Act would limit the power of any grand jury to issue a subpoena. Rather, the government could still use the grand jury to obtain records in terrorism investigations, just as it can in any other investigation of crime, such as drug trafficking or fraud.

While the grand jury's powers are extensive, grand juries are supposed to obtain records that have some relevance to criminal wrongdoing. There is no such requirement in intelligence investigations, which often implicate political activity protected by the First Amendment. As a result, the power to obtain records must be limited in some other way in order to prevent widespread fishing expeditions into the personal records and reading habits of ordinary Americans.

The SAFE Act does this by restoring the requirement of "specific and articulable facts" that the records pertain to a terrorist, spy or other foreign agent. This level of individual suspicion is more than mere relevance, but less than probable cause – the same level a police officer must show to stop and frisk a person on the street. *See Terry* v. *Ohio*, 392 U.S. 1, 30 (1968). This is not a high hurdle to pass – but it does require *some* individual suspicion – and so would greatly limit the danger that the FISA records search power could be misused to secretly obtain the private records of innocent people.

National Security Letters. The SAFE Act contains a simple clarification of the government's power to obtain records without a court order using national security letters. The power to obtain national security letters was amended by section 505 of the USA PATRIOT Act to eliminate the requirement that there be any individual suspicion the records pertain to a foreign agent. National security letters may be issued to obtain, among other things, transactional records about the customers of a telephone, Internet, or other "communications service provider." 18 U.S.C. § 2709(b).

The SAFE Act does not restore the individual suspicion requirement or otherwise amend the general standards for national security letters provided the USA PATRIOT Act, and now greatly expanded by the amended definition of "financial records" in the Intelligence Act for FY2004.[5] It does clarify the law to ensure that libraries are not treated as "communications service providers" subject to providing transactional records about their patrons simply because they provide public access to the Internet. This change is needed to ensure that the amendments to section 215 have the desired effect of safeguarding the privacy of library records.

Libraries occupy a unique and important role in our democratic society. It is not asking too much to require the government to obtain information about the reading habits or Internet usage of library patrons only by presenting a grand jury subpoena, FISA records order based on individual suspicion, or other court order. A national security letter is not a court order and is not reviewed by an impartial person, such as a judge or magistrate, before it is issued. The Attorney General's letter fails to acknowledge that the Justice Department could obtain the information it might need from a library with any number of authorities – it simply could not do so outside the supervision of a court.

The letter also mischaracterizes the effect of this provision by claiming that it treats use of the Internet in a library differently than use of the Internet in a home or business.

[5] The SAFE Act's expanded sunset provision includes section 505 of the USA PATRIOT Act. As a result, if the SAFE Act passed, Congress would have to consider whether to restore that requirement by allowing that provision to expire at the end of 2005.

Under the SAFE Act, a library would be treated precisely the same as any other *customer* of a communications service provider. Records held by the communications service provider about a library's account – or about the account of an individual who uses a library computer to access their own Internet account – could be obtained with a national security letter just as such records could be obtained about the account of any other home or business customer. The SAFE Act merely makes clear that the library itself cannot be regarded as a communications service provider.

Sunsets. Adding new provisions to the sunset clause makes common sense because it gives Congress much-needed leverage in its oversight of the Administration's anti-terrorism effort – a point the Attorney General's letter conveniently ignores.

The Administration is on record opposing the sunsetting of any provision of the USA PATRIOT Act. Congress has wisely rejected that position despite repeated calls by the Administration to eliminate the sunsets early, because it expected that the leverage of the sunset clause (section 224) would encourage Justice Department cooperation with oversight efforts.

The continued failure of the Justice Department to answer many of Congress's legitimate questions shows that Congress was right to be worried its oversight efforts would not be taken seriously. Questions have gone answered for lengthy periods of time, and some information requested by members in their oversight capacity has been provided on a fragmentary basis or not at all. Without the sunset provision, it seems likely that the Justice Department's cooperation with oversight efforts would be even more cursory.

Most of the USA PATRIOT Act 158 provisions are not subject to the sunset clause. Congress chose to limit the sunset clause to some 14 surveillance provisions that it believed could pose a serious risk to personal privacy. Unfortunately, Congress omitted a number of key provisions, including those broadening "sneak and peek" searches, nationwide search warrants, and national security letters. The inclusion of these four additional provisions within the sunset clause does not prejudice, one way or another, the decision Congress must make by December 31, 2005 about whether to reauthorize these or other provisions of the USA PATRIOT Act.

Conclusion. The Attorney General's letter on the SAFE Act is based on hyperbole and mischaracterization of the Act's provisions, not facts. The SAFE Act takes away none of the government's powers under the USA PATRIOT Act, and certainly does not take away any of its pre 9/11 terrorism powers. Instead, the Act merely restores some measure of judicial and Congressional oversight to particularly sensitive surveillance authorities. Congress should enact the SAFE Act this year.

SAFE Act: PATRIOT Surveillance Powers Compared

surveillance power	*before 9/11*	*now*	*SAFE Act*
Roving wiretaps under the Foreign Intelligence Surveillance Act (FISA).		✓	✓
	No roving wiretaps under FISA, but were available for criminal investigations (including for terrorism). Criminal roving taps require that target of search is specified and agents "ascertain" that target is using the facility.	Now there are FISA roving wiretaps, but unlike criminal roving wiretaps, FISA roving wiretaps do not need to specify target and agents need not ascertain target is using that telephone. **PATRIOT § 206; Intelligence Act for FY2002 § 314.**	Would keep FISA roving wiretaps, but they would have to observe same requirements as criminal roving wiretaps, i.e., they must (1) specify a target, and (2) would have to ascertain target is using that facility. **SAFE § 2**
"Sneak and peek" – criminal search warrants with delayed notice.	✓	✓	✓
	Some courts had approved in specific circumstances, despite lack of statutory authority. Two circuit courts of appeals imposed presumptive seven-day limit on delaying notice.	Now there is statutory authority for sneak and peek searches under wide-ranging circumstances, including whenever notice could "seriously jeopardize" a prosecution. No time limit for delaying notice **PATRIOT § 213**	Would limit statutory reasons for delaying notice to three specific harms – danger to persons, flight from prosecution, or destruction of evidence – and imposes a seven-day limit, which court can renew **SAFE § 3**
Library and other personal records searches under FISA.		✓	✓
	FISA search orders were available only for certain travel-related "business" records (not library or personal records) where FBI has "specific and articulable facts" connecting records to foreign agent.	Now these orders are available for any and all records, including library records, without individual suspicion. **PATRIOT § 215**	Would still be available for any and all records – including library records – but only where FBI has "specific and articulable facts" connecting records to foreign agent. **SAFE § 4**

SAFE Act: PATRIOT Surveillance Powers Compared

surveillance power	*before 9/11*	*now*	*after SAFE*
National security letters (no court order required) for financial records, telephone and ISP bills, consumer credit reports.	✓ Were available only where FBI could show "specific and articulable facts" connecting records to foreign agent.	✓ Now available without individual suspicion; definition of "financial records" greatly expanded. **PATRIOT § 505; Intelligence Act for FY2004 § 334.**	✓ Would still be available without individual suspicion, but libraries with Internet terminals would not be subject to national security letters. **SAFE § 5**
Sunset clause.	not applicable	Now applies to 14 provisions (out of 158 total). **PATRIOT § 224**	Would be expanded to include four additional provisions, for a total of 18 (out of 158 total). **SAFE § 6**