Analysis of Sensenbrener-Conyers Bill (10/2/01)

This memorandum summarizes the changes that the October 1, 2001 Sensenbrenner-Conyers "PATRIOT Act of 2001" would make to title I of the September 21, 2001 version of the Administration's draft "Anti-Terrorism Act" (ATA). Items 2 and 5 seek to address issues raised by the NetCoalition. This memo was prepared by Piper Marbury Rudnick & Wolfe LLP exclusively to analyze the differences between Chairman Sensenbrenner's draft and the ATA, and in no way reflects on the substance of the ATA that is not subject to the changes in the Sensenbrenner draft.

1. Section 101(c)—Definitions of Pen Register and Trap and Trace Device—Banning Acquisition of Contents of the Communication

Change

The definitions of "pen register" and "trap and trace device" in ATA §101(c) are limited by adding language to clarify that the amended definitions would not include the "contents of such communications."

Implication

The intent of this provision appears to be to clarify that, in extending pen registers and trap and trace devices to cover Internet communications, the communications tracing authorization does not extend to acquisition of the contents of the targeted communications. It leaves open the issue of whether the tracing authority applies only to the acquisition of information about the destination and termination of the Internet communications. It is unclear whether this section covers URLs.

2. Section 101(d)—Nationwide Service of Pen Register and Trap and Trace Device Court Orders—Limiting Liability for Unnamed Service Providers

Change

18 U.S.C. § 3124(d), the pen register immunity provision which states that no cause of action shall lie against service providers that provide "information, facilities, or assistance in accordance with the terms of a court order," is amended by striking "the terms of" after "in accordance with."

Implication

This change is part of a package of amendments requested by NetCoalition and others that is intended to clarify that providers who are not named in nationwide pen register and trap and trace court orders are nonetheless protected from liability for complying with them. The change proposed by the Sensenbrenner bill only removes a limitation that restricts the applicability of the immunity provision to conduct specified by "the terms of" the court order—which are expected increasingly not to name the service providers upon whom the orders will be served. Industry has requested additional language whereby service providers may request law enforcement to accompany such

court orders with a written certification confirming that the order applies to the entity being served.

3. Section 103—Scope of Executive Branch Officials Authorized to Receive Information Obtained Via Wiretaps—Narrowing of Expansion

Change

The scope of the amendment in Section 103 on Authorized Disclosure is narrowed in two ways: (a) limiting the expansion of authorized disclosures for purpose of section 2517 only "as it relates to foreign intelligence information" and (b) limiting the categories of personnel from "any officer or employee of the executive branch of the Federal Government" to "any Federal law enforcement, intelligence, national security, national defense, protective, immigration personnel, or the President or Vice President of the United States."

Implication

The ATA's proposed section on authorized disclosures would have permitted broad disclosure of information obtained from wiretaps to all employees of the executive branch without limitation on purpose. This amendment limits disclosure to law enforcement, national security and other directly relevant individuals and limits the disclosures to foreign intelligence information.

4. Use of Wiretap Information Obtained from Foreign Governments in Violation of Fourth Amendment Principles—Deleted

Change

The Sensenbrenner bill would drop the ATA's Section 105 "Use of Wiretap Information from Foreign Governments."

Implication

ATA section 105 had been included to codify the "silver platter" principle that United States prosecutors could use against defendants information collected by a foreign government even if the collection would have violated the Fourth Amendment. Although the proposed language ("without knowing participation" of American law enforcement personnel) probably would have exceeded the contours of the "silver platter" principle, law enforcement can still rely upon it in prosecutions because the principle still exists in case law.

5. Section 105(3)—Computer Trespasser Communications—Good Faith Defense for Compliance with Wiretap Authority Added

Change
§105(3) would expand the good faith defense in 18 U.S.C. § 2520(d)(3) to read "a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of."

Implication
This attempts to protect the owner or operator of a protected computer who, under Section 105 (ATA § 106), authorizes a law enforcement agent to intercept the communications of a trespasser. Although ATA § 106 would protect law enforcement when an owner or operator of a protected computer authorizes the interception of the communications of a trespasser, it does not appear to protect the owner or operator from liability for authorizing such an interception, for example, if it errs in good faith in identifying the trespasser. Under the "switchboard" provision of existing law (18 U.S.C. § 2511(2)(a)(i)), a service provider can intercept or disclose a user's communications when "necessary . . . to the protection of the right or property of the provider." But there is case law indicating that the good faith defenses are not a basis for avoiding liability where actions are taken on the basis of an erroneous belief that a statutory provision authorizes the action. This section would extend the good faith defense to apply to a service provider's belief that the "switchboard" provision permits them to authorize a law enforcement agent to intercept the communications of a trespasser. It addresses a concern raised by the NetCoalition.

6. Section 109—Conflict Between Cable Act and ECPA Clarification

Change
Section 109 was changed to clarify that the Cable Act's privacy provisions "shall not apply" to voluntary or obligatory disclosures of information (other than "information revealing customer cable viewing activity") made under the wiretap statutes (ECPA). In the administration's draft, the language provided that "nothing shall be deemed to restrict" voluntary or obligatory disclosures.

Implication
This change addresses one of the problems raised by the ATA's proposal, which is its potential failure to supercede the cable operator's obligation to notify the subscriber as a condition precedent to disclosing the information requested by a court order. However, the Sensenbrenner proposal continues the ATA's attempt to carve out "information revealing customer cable viewing activity" from the disclosures no longer subject to the Cable Act. This could create ambiguity when Internet services are provided over a cable

facility. For example, section 107's proposed new requirements for production of records revealing "session times and duration" could conflict with section 109's exception for "viewing activity." The new legislation needs to clarify the law, not add to the confusion about the obligations of a cable operator providing Internet services over cable facilities. The House Commerce Committee is marking up a bill that should resolve this issue. Apparently, the Judiciary Committee has agreed to this approach.

7. Section 110—Emergency Disclosure of Electronic Communications to Protect Life and Limb

Change

Section 110(b)(4) would expand the immunity provisions for a service provider's disclosure of stored communications (r other surveillance assistance in connection with such communications) to add conduct undertaken in accordance with a "statutory authorization" to the list of actions taken pursuant to "court order, warrant, subpoena, or certification under this chapter."

Implication

This expansion of the immunity provision (requested by WorldCom), coupled with the other provisions of Section 110, would help resolve an ambiguity in current law that inhibits service providers from disclosing customer information in emergency situations involving death or serious physical injury. The heart of section 110 would authorize service providers to disclose the content of stored e-mail messages and other customer information where the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information." The additional language in the Sensenbrenner bill would clarify that such decisions by service providers are immune from suit.

8. Section 111—Statutory Exclusionary Rule—Modification

Change

Section 111 of the Sensenbrenner proposal would amend ECPA's statutory exclusionary rule in two ways. First, it would expand 18 U.S.C. § 2515 to cover the contents of electronic communications regardless of whether obtained in "real time" (interception) or from electronic storage. Second, it would deny persons charged with wiretapping from the benefits of this statutory exclusionary rule.

Implication

The expansion of the scope of ECPA's statutory exclusionary rule is a change long sought by the civil liberties community. The carve out for cases prosecuting wiretapping

offenses is presumably necessary to introduce evidence of the defendant's illegal wiretapping activities. ATA did not contain a corresponding provision.

9. Section 112—Reports Concerning the Disclosure of Contents of Electronic Communications

Change

Section 112 of the Sensenbrenner proposal would add a new subsection to the end of 18 U.S.C. § 2703 that would require annual reporting of surveillance conducted in connection with the government's acquisition of the contents of stored communications (i.e., subsections (a) and (b) of section 2703). It would accomplish this by requiring judges, other issuing authorities, and the Attorney General to report, on an annual basis, to the Administrative Office of the United States Courts on each order, warrant, or subpoena issued pursuant to subsections (a) and (b) of section 2703, and requiring the Administrative Office to compile this data and make annual reports to Congress about these types of surveillance.

Implication

The new proposal would require annual reports for this type of surveillance similar to the annual reports that are already made in connection with wiretaps (interceptions in "real time") and pen register and trap and trace devices. These annual reports help with congressional oversight and public accountability. ATA did not contain a corresponding provision.

10. Section 153—"Foreign Intelligence Information" Test—Modification

Change

Section 153 would change 50 U.S.C. § 1804 to provide that the applications for court orders under FISA would have to include certification by the Assistant to the President for national security affairs or an executive official that, among other things, "a *significant* purpose of the surveillance is to obtain foreign intelligence information." The administration's proposal would require a certification to state only that "a purpose" of the surveillance is to obtain foreign intelligence information.

Implication

Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This would lower the barriers to surveillance under FISA, but not lower them as much as requested by the Administration.

11. Section 154—Foreign Intelligence Information Sharing—Narrowing of Expansion

Change
Section 154 would clarify that the provision of foreign intelligence information to the listed individuals must be "for the performance of official duties."

Implication
The ATA proposes to authorize the sharing of foreign intelligence information obtained in criminal investigations to be shared with certain other Executive Branch officials who are defined by their job description. The Sensenbrenner bill would further specify that such officials could receive the information only "for the performance of official duties."

12. Section 156—Business Records—Modification of Standard

Change
Instead of authorizing the government to compel the production of business records under an administrative subpoena as proposed by ATA §156, the Sensenbrenner bill would still require the Director of the FBI or a designee to apply to a FISA judge for a court order to obtain business records.

Implication
The Administration's proposal would have replaced the existing formal court order proceeding with a generic "administrative subpoena" authority for business records under FISA. The Sensenbrenner change would preserve the court order process for obtaining business records under FISA, but would provide for less restrictive standards for issuance of the court order.

13. Section 157—Deletion of Proposed Change to Allow Lower Ranking FBI Agent Ability To Obtain National Security Letter

Change
Section 157 would strike from ATA § 157 the proposal that would have permitted the FBI special agents in charge of bureau field offices to authorize surveillance pursuant to a National Security Letter (NSL).

Implication
The Administration contends that the procedures for NSLs are so burdensome that "they often take months to be issued." The Sensenbrenner change would preserve the thrust of the Administration's efforts to streamline the process for obtaining NSL authority, but would leave in place the current law's requirement that the NSL have the signature of a high-ranking official at FBI headquarters.

14. Sections 160 and 158—Sunset Provisions

Change

New section 160 of the Sensenbrenner bill would sunset, with 2 exceptions, the surveillance and intelligence gathering provisions (all of Title I) of the bill. (One exception would apply section 109 clarifying the surveillance cooperation obligations of cable operators. Another exception would apply to section 159 relating to restoring presidential authorities to confiscate the property of enemies and enabling courts in confiscation proceedings to consider classified evidence ex parte and in camera.[*]) New section 158 would direct the President to propose legislation by August 31, of 2003 for the provisions that will sunset.

***

For more information, contact Ron Plesser, Jim Halpert, or Milo Cividanes at (202) 861-2900

[*] This memo does not discuss the substantial revisions that the Sensenbrenner bill makes to section 159 of ATA.