THE U.S. PATRIOT ACT of 2001 CHANGES TO ELECTRONIC SURVEILLANCE LAWS

Bryan R. Lemons
Branch Chief

Shortly after the terrorist attacks that occurred on September 11, 2001, Congress passed the "**U**niting and **S**trengthening America by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism," commonly referred to as the "U.S. Patriot Act of 2001." The purpose of this article is to highlight some of the resulting major changes in electronic surveillance laws. This article is not intended to be a comprehensive summary of all of the changes brought by the legislation.

TERRORISM AS A PREDICATE OFFENSE

Title 18 U.S.C. § 2516 lists the predicate offenses for which wire, oral, or electronic intercept orders may be authorized, upon a showing of probable cause to believe the offense is being committed. "The offenses that may be the predicate for a wire or oral interception order are limited to only those set forth in … § 2516(1)."[1] With passage of the "U.S. Patriot Act," crimes "relating to terrorism" have now been made predicate acts for wire or oral interception orders, as have offenses "relating to chemical weapons."[2]

[1] *United States Attorney's Manual*, Title 9, Criminal Resource Manual 28.
[2] Title 18 U.S.C. § 2516(1)(q)

PEN REGISTERS AND TRAP AND TRACE DEVICES

Title 18 U.S.C. §§ 3121 – 3127 outline the federal requirements for use of pen registers and trap and trace devices.[3] Prior to passage of the "U.S. Patriot Act," the statutory definitions of these two devices did not explicitly allow for their use to capture Internet communications, such as capturing the "To" and "From" information contained in an e-mail header. The "U.S. Patriot Act" modified these definitions, and they now expressly authorize utilization of pen registers and trap and trace devices on Internet communications. Further, Title 18 U.S.C. § 3123(a) previously allowed for the issuance of a court order authorizing a pen register or trap and trace device only "within the jurisdiction" of the issuing court. The "U.S. Patriot Act" now allows for a court to issue a single order that is valid "anywhere within the United States."[4]

VOICE MAIL STORED WITH THIRD PARTY PROVIDER

Title 18 U.S.C. § 2510(1) included within its definition of "wire communication" the phrase "any electronic storage of such communication." Additionally, the Electronic Communications Privacy Act of 1986 (ECPA) addressed law enforcement access to stored "electronic"

[3] "A pen register records outgoing addressing information (such as a number dialed from a monitored telephone), and a trap and trace device records incoming addressing information (such as caller ID information)." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 148, Computer Crime and Intellectual Property Section, Criminal Division, Department of Justice (2001)
[4] Title 18 U.S.C. § 3123(a)(1)

communications held by a third party provider, but not stored "wire" communications. Thus, voice mail stored with a third party provider could not be obtained by a law enforcement officer with a search warrant (as could "electronic communications"), but required a Title III interception order. The "U.S. Patriot Act" amended the ECPA, and now authorizes law enforcement officers to use search warrants to compel disclosure of voice mail stored with a third party provider. This provision of the "U.S. Patriot Act" will expire on December 31, 2005.

COMPUTER HACKING INVESTIGATIONS

Prior to passage of the "Patriot Act," investigators were not permitted to obtain interception orders for wire communications in computer hacking investigations. Title 18 U.S.C. § 2516(1) has now been amended to include violations of Title 18 U.S.C. § 1030 (Computer Fraud and Abuse) as predicate offenses. However, this provision of the "U.S. Patriot Act" will expire on December 31, 2005.

OBTAINING INFORMATION FROM THIRD PARTY PROVIDERS WITH A SUBPOENA

Title 18 U.S.C. § 2703 outlined the information a law enforcement officer could obtain with a subpoena from a third party provider of electronic communication (e.g., AOL). Termed "basic subscriber information," it included a customer's name, address, local and long distance telephone toll billing records, etc.[5] Other types of information, such as credit card numbers used, could only be obtained with a search warrant or § 2703(d) court order. The "U.S. Patriot Act" expands "basic subscriber information" to now include "means and source of payment for such service (including any credit card or bank account number)," "records of session times and durations," and "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address."[6]

SEARCH WARRANTS FOR WIRE AND ELECTRONIC COMMUNICATIONS HELD BY THIRD PARTY PROVIDER

Prior to passage of the "U.S. Patriot Act," the ECPA required that law enforcement officers use a search warrant to compel a third party provider of electronic communications to disclose communications in storage "for one hundred and eighty days or less."[7] Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, only a court in the district where the actual communication was located could issue this search warrant. Now, any court "with jurisdiction over the offense under investigation" can issue a nationwide search warrant for communications stored by third party providers, regardless of where the communication is physically located. And, as noted in paragraph III, above, "wire communications" are now covered by this rule. This provision of the "U.S. Patriot Act" will expire on December 31, 2005.

DELAYED NOTICE OF SEARCH WARRANTS

Title 18 U.S.C. § 3103a has been amended to permit law enforcement

[5] Title 18 U.S.C. § 2703(C)

[6] Title 18 U.S.C. § 2703(c)(2)

[7] Title 18 U.S.C. § 2703(a)

officers to delay notice of the execution of a search warrant in special circumstances. Specifically, § 3103a permits notice to be delayed in situations where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result." An "adverse result" is defined as (a) endangering the life or physical safety of an individual; (b) flight from prosecution; (c) destruction of or tampering with evidence; (d) intimidation of potential witnesses; or (e) otherwise seriously jeopardizing an investigation or unduly delaying a trial."[8]

[8] Title 18 U.S.C. § 2705(a)(2)