

even foreign intelligence crimes — to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.

## 6. THE USA-PATRIOT ACT

On September 11, 2001, terrorists hijacked four planes and crashed three of them into the World Trade Center and the Pentagon, killing thousands of people. The nation was awakened into a world filled with new frightening dangers, and shortly after the September 11 attacks, letters laced with the deadly bacteria Anthrax were sent in the mails to several prominent individuals in the news media and in politics. Acting with great haste, Congress passed a sweeping new law expanding the government's electronic surveillance powers in many significant ways. Called the "Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act" (USA-PATRIOT Act), the Act made a number of substantial changes to federal wiretap law, FISA, FERPA, immigration law, and money laundering statutes. The discussion below will focus on the changes that pertain to information privacy law, with particular emphasis on federal wiretap law and FISA.<sup>34</sup>

**Definition of Terrorism.** Section 802 of the USA-PATRIOT Act added to 18 U.S.C. § 2331 a new definition of "domestic terrorism." According to the Act, domestic terrorism involves "acts dangerous to human life that are a violation of the criminal laws of the United States or of any State" that "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 . . . occur primarily within the territorial jurisdiction of the United States." According to many proponents of civil liberties, this definition is very broad and could potentially encompass many forms of civil disobedience, which, although consisting of criminal conduct (minor violence, threats, property damage), includes conduct that has historically been present in many political protests and has never been considered to be terrorism.

**Delayed Notice of Search Warrants.** Under the Fourth Amendment, the government must obtain a warrant and provide notice to a person before conducting a search or seizure. Case law provided for certain limited exceptions. Section 213 of the USA-PATRIOT Act adds a provision to 18 U.S.C. § 3103a, enabling the government to delay notice if the court concludes that there is "reasonable cause" that immediate notice will create an "adverse result" such as physical danger, the destruction of evidence, delayed trial, flight from prosecution, and other circumstances. § 3103a(b). This provision does not sunset. Warrants enabling a covert search with delayed notice are often referred to as "sneak and peek" warrants. Civil libertarians consider "sneak and peek" warrants dan-

---

<sup>34</sup>For more background about the USA-PATRIOT Act, see Steven A. Osher, *Privacy, Computers, and the Patriot Act: The Fourth Amendment Isn't Dead, But No One Will Insure It*, 54 Fla. L. Rev. 521 (2002); Sharon H. Rackow, Comment, *How the USA PATRIOT Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. Pa. L. Rev. 1651 (2002).

gerous because in a covert search, the individual cannot safeguard her rights and there is little supervision of the government's carrying out of the search.

***Shifting Stored Wire Communications from Title I to Title II.*** Under Title I of federal wiretap law, the definition of wire communications consisted of the temporary storage of such communications. As a result, obtaining access to certain stored wire communications, such as voicemail, was considered an "intercept" under Title I rather than accessing stored communications under Title II. See *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1986) (holding that the retrieval of a voicemail message was an interception governed by Title I). Likewise, if a stored e-mail had a voice attachment, Title I's strict court order requirements applied rather than Title II's more relaxed requirements. The USA-PATRIOT Act (§209) deleted "electronic storage" from the definition of wire communications, making stored wire communications fall under Title II. This provision will sunset on December 31, 2005.

***Increased Number of Subscriber Records Obtainable Under Title II.*** Under Title II of federal wiretap law, §2703(c), the government could obtain only certain subscriber records from a communications service provider: name, address, length of service, means of payment, and so on. Section 210 of the USA-PATRIOT Act adds new records to this list, including "records of session times and durations," "any temporarily assigned network address," and "any credit card or bank account number" used for payment. §2703(c)(2).

***New Definition of Pen Registers and Trap and Trace Devices.*** Under Title III of the ECPA, §3121 *et seq.*, the definitions of pen registers and trap and trace devices focus primarily on telephone numbers. Thus, a pen register is defined under 18 U.S.C. §3127(3) as:

a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. . . .

Section 216 of the USA-PATRIOT Act changed the definition to read:

a device or *process* which records or decodes *dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication* is attached. . . (changes emphasized).

These changes alter the definition of a pen register from applying not only to telephone numbers but also to Internet addresses, e-mail addressing information (the "to" and "from" lines on e-mail), and the routing information of a wide spectrum of communications. The inclusion of "or process" after "device" enlarges the means by which such routing information can be intercepted beyond the use of a physical device. The definition of a trap and trace device was changed in a similar way. These provisions do not sunset.

Recall that under Title III, a court order to obtain such information does not require probable cause, but merely certification that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. §3123. The person whose communications

are subject to this order need not even be a criminal suspect; all that the government needs to certify is relevance to an investigation.

Recall *Smith v. Maryland* earlier in this chapter where the Court held that pen registers were not protected under the Fourth Amendment. Does the new definition of pen register and trap and trace device under the USA-PATRIOT Act go beyond *Smith v. Maryland*? Are Internet addresses and e-mail addressing information analogous to pen registers? Or are they different? Note that Internet addresses reveal how a person navigates the Internet. Based on *Smith v. Maryland*, does the Fourth Amendment apply to such information? If the government were to obtain e-mail header information or Internet addresses through a Title III order, is such information properly obtained under the Fourth Amendment?

***Nationwide Scope of Pen Register/Trap and Trace Orders.*** Originally, pen register/trap and trace orders were only valid within the jurisdiction of the court issuing the order. The USA-PATRIOT Act, § 216, permits the court having jurisdiction over the crime under investigation to issue pen register/trap and trace orders that are valid throughout the nation. This provision applies to all crimes, not just terrorism, and may place a significant burden on smaller ISPs to challenge in court the scope and duration of the order.

***Nationwide Scope of Search Warrants for E-Mail.*** For warrants to obtain stored e-mail less than 180 days old under Title II of the ECPA, § 2703(a), § 220 of the USA-PATRIOT Act permitted the court having jurisdiction over a crime to issue a warrant applying beyond the court's jurisdiction to anywhere in the nation. This provision will sunset on December 31, 2005.

***Expansion of Application of FISA.*** Prior to the USA-PATRIOT Act, FISA applied when foreign intelligence gathering was "the purpose" of the investigation. The USA-PATRIOT Act (§ 204) changed this language to make the FISA applicable when foreign intelligence gathering is "a significant purpose" of the investigation. § 50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B).

***Sharing of Foreign Intelligence Information.*** Section 203 of the USA-PATRIOT Act permits extensive sharing of foreign intelligence information among various law enforcement entities and intelligence agencies. The purposes for which the information can be shared are defined very broadly: "to assist the official who is to receive that information in the performance of his official duties."

***Roving Wiretaps Under FISA.*** Section 206 of the USA-PATRIOT Act amended the FISA to allow the interception of communications beyond "specified person[s]." Previously, the FISA, 50 U.S.C. § 1805(c)(2)(B) provided that an order approving electronic surveillance shall direct

that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such

carrier, landlord, custodian, or other person is providing that target of electronic surveillance.

As amended by the USA-PATRIOT Act, the provision reads:

that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance (changes emphasized).

**Private Right of Action for Government Disclosures.** The USA-PATRIOT Act adds a provision to Title II of federal wiretap law which provides for civil actions against the United States for any "willful" violations. 18 U.S.C. § 2712. The court may assess actual damages or \$10,000 (whichever is greater) and litigation costs. Such an action must first be presented before the "appropriate department or agency under the procedures of the Federal Tort Claims Act."

**Changes to FERPA and the Cable Act.** These changes will be discussed later on in Chapter 6, when these Acts are discussed.

## C. ENCRYPTION

Encryption includes the ability to keep communications secure by concealing the contents of a message. With encryption, even if a communication is intercepted, it still remains secure. Encryption works by translating a message into a code of letters or numbers called "cypher text." The parties to the communication hold a *key*, which consists of the information necessary to translate the code back to the original message, or "plain text." Since ancient times, code-makers have devised cryptographic systems to encode messages. But along with the code-makers arose code-breakers, who were able to figure out the keys to cryptographic systems by, for example, examining the patterns in the encoded messages and comparing them to patterns in a particular language and the frequency of use of certain letters in that language. Today, computers have vastly increased the complexity of encryption.

Encryption presents a difficult trade-off between privacy and security. It is an essential device to protect the privacy of electronic communications in an age where such communications can so easily be intercepted and monitored. On the other hand, it enables individuals to disguise their communications from detection by law enforcement officials.<sup>35</sup> As Whitfield Diffie and Susan Landau observe:

<sup>35</sup>For more background on encryption, see Simon Singh, *The Code: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (1999); Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (2002); A. Michael Froomkin, *The Met-*